IEEE 3000
STANDARDS COLLECTION™

IEEE 3006 STANDARDS:
POWER SYSTEMS RELIABILITY

IEEE Std 3006.7™-2013

IEEE Recommended Practice for Determining the Reliability of 7×24 Continuous Power Systems in Industrial and Commercial Facilities

IEEE STANDARDS ASSOCIATION

IEEE

IEEE Recommended Practice for Determining the Reliability of 7x24 Continuous Power Systems in Industrial and Commercial Facilities

Sponsor

Technical Books Coordinating Committee
of the
IEEE Industry Applications Society

Approved 6 March 2013

IEEE-SA Standards Board

Recognized as an American National Standard

Abstract: Methods for determining the reliability of 7×24 continuous power systems in industrial and commercial facilities are described in this recommended practice. The method of reliability analysis by probability methods is described first. This is followed by a discussion of how to evaluate the results and how to implement changes to ensure that the expected degree of reliability is achieved.
Keywords: availability, failure rate, fault tree analysis, IEEE 3006.7™, mean time between failure, mean time to repair, reliability, reliability block diagram

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-7381-8275-9 STD98164
Print: ISBN 978-0-7381-8276-6 STDPD98164

Notice and Disclaimer of Liability Concerning the Use of IEEE Documents: IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon any IEEE Standard document.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Translations: The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official Statements: A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on Standards: Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important to ensure that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE working group at http://standards.ieee.org/develop/wg/.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Photocopies: Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Notice to users

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://standards.ieee.org/index.html or contact the IEEE at the address listed previously. For more information about the IEEE Standards Association or the IEEE standards development process, visit IEEE-SA Website at http://standards.ieee.org/index.html.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE recommended practice was completed, the Power Systems Reliability (PSR) Working Group had the following membership:

Robert Arno, *Chair*

William Braun
Timothy J. Coyle
Neal Dowling
Peyton Hale
Masoud Pourali
Robert J. Schuerger
Michael Simon
Christopher C. Thompson, Jr.
Joseph Weber

At the time this recommended practice was submitted by the PSR Working Group to the IEEE-SA Standards Board for approval, the 3006.7 Working Group had the following membership:

Robert J. Schuerger, *Chair*

Robert Arno
Jose Cay II
Raymond Chiu
Edwin Cothran
Ann'claude Coutu
Neal Dowling
Addam Friedl
Joaquin Fuster
Gardson Githu
Peter Gross
Ian Levine
Michael Simon
Sonny K. Siu

The following members of the individual balloting committee voted on this recommended practice. Balloters may have voted for approval, disapproval, or abstention.

William Ackerman
Robert Arno
Adam Bagby
Wallace Binder
Frederick Brockhurst
Gustavo Brunello
William Bush
William Byrd
Paul Cardinal
Keith Chow
Donald Colaberardino
Bryan Cole
Larry Conrad
Stephen Conrad
Terry Conrad
Carey Cook
Jesus DeLeon Diaz
Douglas Dorr
Randall Dotson
Neal Dowling
Stephen Fairfax
Keith Flowers
Carl Fredericks
Doaa Galal
Randall Groves
Thomas Gruzs
Ajit Gwal
Scott Hietpas
Werner Hoelzl
Mayank Jain
Laszlo Kadar
Piotr Karocki
Gael Kennedy
Yuri Khersonsky
Yoonik Kim
Jim Kulchisky
Saumen Kundu
Wei-Jen Lee
Greg Luri
Ahmad Mahinfallah
Wayne Manges
John McAlhaney, Jr.
John Merando
Edrin Murzaku
Daniel Neeser
Dennis Neitzel
Michael S. Newman
Joe Nims
Gearold O. H. Eidhin
Lorraine Padden
Richard Paes
Mirko Palazzo
Sergio Panetta
Masoud Pourali
Louie Powell
Moises Ramos
Daniel Leland Ransom
John Roach
Michael Roberts
Charles Rogers
Vincent Saporita
Bartien Sayogo
Robert J. Schuerger
Robert Seitz
Gil Shultz
Michael Simon
David Singleton
James Smith
Jerry Smith
Chandrasekaran Subramaniam
Peter Sutherland
David Tepen
Marcelo Valdes
Kenneth White
James Wikston
Jian Yu

When the IEEE-SA Standards Board approved this recommended practice on 6 March 2013, it had the following membership:

John Kulick, *Chair*
David J. Law, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi	Mark Halpin	Ron Petersen
Peter Balma	Gary Hoffman	Gary Robinson
Farooq Bari	Paul Houzé	Jon Walter Rosdahl
Ted Burse	Jim Hughes	Adrian Stephens
Wael William Diab	Michael Janezic	Peter Sutherland
Stephen Dukes	Joseph L. Koepfinger*	Yatin Trivedi
Jean-Philippe Faure	Oleg Logvinov	Phil Winston
Alexander Gelman		Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Julie Alessi
IEEE Standards Program Manager, Document Development

Lisa Perry
IEEE Standards Program Manager, Technical Program Development

Introduction

This introduction is not part of IEEE Std 3006.7-2013, IEEE Recommended Practice for Determining the Reliability of 7x24 Continuous Power Systems in Industrial and Commercial Facilities.

IEEE 3000 Standards Collection™

This recommended practice was developed by the Technical Books Coordinating Committee of the Industrial and Commercial Power Systems Department of the Industry Applications Society as part of a project to repackage the popular IEEE Color Books®. The goal of this project is to speed up the revision process, eliminate duplicate material, and facilitate use of modern publishing and distribution technologies.

When this project is completed, the technical material in the thirteen IEEE Color Books will be included in a series of new standards—the most significant of which will be a new standard, IEEE Std 3000™, IEEE Recommended Practice for the Engineering of Industrial and Commercial Power Systems. The new standard will cover the fundamentals of planning, design, analysis, construction, installation, startup, operation, and maintenance of electrical systems in industrial and commercial facilities. Approximately 60 additional dot standards, organized into the following categories, will provide in-depth treatment of many of the topics introduced by IEEE Std 3000™:

— Power Systems Design (3001 series)

— Power Systems Analysis (3002 series)

— Power Systems Grounding (3003 series)

— Protection and Coordination (3004 series)

— Emergency, Standby Power, and Energy Management Systems (3005 series)

— Power Systems Reliability (3006 series)

— Power Systems Maintenance, Operations, and Safety (3007 series)

In many cases, the material in a dot standard comes from a particular chapter of a particular IEEE Color Book. In other cases, material from several IEEE Color Books has been combined into a new dot standard.

This recommended practice is an update and expansion of the material in Chapter 8 of IEEE Std 493™ (*IEEE Gold Book™*).

IEEE Std 3006.7™

The explosive growth of computer technology has literally changed the way business is conducted. Cell phones, text messaging, and e-mail have become the norm and the Internet provides a communication medium not previously available. Stock trading and banking, along with an incredible diversity of retail sales, occur daily via the Internet.

With the broad expansion of computer technology comes the necessity of providing an infrastructure capable of supporting it. The ITIC susceptibility curve, from IEEE Std 1100™-2005 (*IEEE Emerald Book™*) shows that electronic equipment can be disrupted by a momentary sag of 20 ms. Two voltage immunity standards currently available have it as 10-ms minimum ride-through time; EN55024 from Special International Committee on Radio Interference (CISPR) and International Electrotechnical Commission (IEC) 61000-6-1, 2005-03. Momentary interruptions of the electrical power can have huge financial consequences. Therefore, specialty equipment, such as uninterruptible power supplies

(UPS), emergency generators, and automatic static transfer switches (STSs) are used to supplement utility power.

Initially, special facilities were designed for mainframe computers, used primarily for banking and finance, called *data centers*. As the use of computers broadened and support of the Internet became a significant market, along with divestiture of the telecommunications industry, the term *7×24 facility* became common. This term is derived from the requirement that the facility operates 7 days a week, 24 hours per day.

Contents

IEEE Recommended Practice for Determining the Reliability of 7x24 Continuous Power Systems in Industrial and Commercial Facilities

1. Overview

1.1 Scope

This recommended practice describes how to determine the reliability of 7×24 continuous power systems in industrial and commercial facilities. The method of reliability analysis by probability methods is described first. This is followed by a discussion of how to evaluate the results and how to implement changes to ensure that the expected degree of reliability is achieved.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 1100™-2005, IEEE Recommended Practice for Powering and Grounding Electronic Equipment (*IEEE Emerald Book™*).[1,2]

IEEE Std 493™-2007, IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (*IEEE Gold Book™*).

IEEE Std 3007.2™-2010, IEEE Recommended Practice for Maintenance of Industrial and Commercial Power Systems.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[3]

availability: (A) (general) The ability of an item—under combined aspects of its reliability, maintainability, and maintenance support—to perform its required function at a stated instant of time or over a stated period of time. (B) (As a performance metric for individual components or a system) The long-term average fraction of time that a component or system is in service and satisfactorily performing its intended function. (C) (As a future prediction) The instantaneous probability that a component or system will be in operation at time t.

failure mode: The manner or form by which a particular component or system fails; the way the component or system manifests unacceptable operation.

fault tree analysis (FTA): A systematic, deductive methodology for determining all of the credible ways for a specific undesirable event to occur. The undesirable event to be analyzed is the top event of the fault tree. The fault tree uses Boolean algebra (AND gates, OR gates, etc.) in a graphical representation to show the logical interrelationships between the initiating basic events, such as component failures, and the top event.

inherent availability (Ai): Long-term average fraction of time that a component or system is in service and satisfactorily performing its intended function. Ai considers only downtime for repair of failures. No logistics time, preventative maintenance, etc., is included.

mean time between failures (MTBF): The arithmetic mean of the times (observed or calculated) between random failures of a component or system.

mean time to repair (MTTR or simply r): The mean time to replace or repair a failed component. Logistics time associated with the repair, such as parts acquisitions and crew mobilization, are not included. It can be estimated by dividing the summation of repair times by the number of repairs and, therefore, is practically the average repair time. The most common unit in reliability analyses is hours (h/f).

[1] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[2] IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).
[3] *IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

operational availability (Ao): Long-term average fraction of time that a component or system is in service and satisfactorily performing its intended function. Ao differs from Ai in that it includes all downtime. Included are downtime for the repair of failures, scheduled maintenance, and any logistics time required (such as obtaining the necessary parts and scheduling the technician to perform the repair).

probability of failure: The unreliability of a component or system, the complement of reliability; probability of failure = (1 − reliability).

reliability: The probability that a component or system will perform required functions under stated conditions for a stated period of time R(t), or (for discrete missions) a stated number of demands.

reliability block diagram (RBD): RBD is a block diagram in which the major components are connected together in the same manner as they are in the one-line or piping diagram. Each of the blocks have the failure and repair data for that component included in the block. The junctions connecting the block are set to account for the system redundancy.

single point of failure (SPOF): Any one component, piece of equipment, or function that by failing causes the whole system to fail.

3.2 Acronyms and abbreviations

ASHRAE	American Society of Heating, Refrigeration, and Air Conditioning Engineers
ATS	automatic transfer switch
BMS	building management system
CISPR	Special International Committee on Radio Interference (*in English*)
CWP	condenser water pump
CRAC	computer room air conditioning unit
CRAH	computer room air handling unit
CT	cooling tower
DX	direct expansion
FTA	fault tree analysis
HVAC	heating, ventilating, and air conditioning
IEC	International Electrotechnical Commission
NASA	National Aeronautics and Space Administration
PDU	power distribution unit
PWP	primary chilled water pump
RBD	reliability block diagram
SLA	service level agreements

SPOF	single point of failure
SBS	static bypass switch
STS	static transfer switch
SWP	secondary chilled water pump
UPS	uninterruptible power supply

4. Special terminology and equipment for 7×24 facilities

Some special terminology has been developed for 7×24 facilities to help in describing systems, determining capacity, and various other issues involved with continuous operation.

4.1 Special terminology for 7×24 facilities

4.1.1 N + 1 designation for equipment

In order to keep critical distribution systems in operation, there are often more of the key components provided than what are required based on system capacity. Redundancy, in general, means creation of new parallel paths in the system structure to improve its reliability. In a system with redundancy, there are more infrastructure components for the critical equipment (such as generators and uninterruptible power supply [UPS] modules) provided than are required to support the total load.

When discussing redundancy of a system, it is common to refer to what is required as "N" (for number). If a facility has two of a particular component, and both are required to carry the critical load, N = 2. If a third component was added, the redundancy would become "N+1." Figure 15 shows an N+1 design in which N = 2 for the generators and N = 4 for the UPS system.

In order to raise the reliability of the system beyond what is possible by adding redundant components, a redundant system is often added. If one system is required to carry the critical load and two complete systems have been provided, that is referred to as "2N." Figure 16 shows a 2N design in which N = 2 for the generators and N = 4 for the UPS system.

4.1.2 Capacity and load density of the data center load

A common metric used to discuss the capacity and load density of the data center is watts per square foot. In metric units, it is watts per square meter. Calculating the watts per square foot is the total usable UPS capacity in watts divided by the total square feet of the data center raised floor (for facilities that have one) or white space (room for IT equipment, often with a white or light colored floor). It varies to some degree how the area of the data center is calculated. The most common method is gross square feet of the data center rooms.

The other method is in watts per rack where the total usable UPS capacity in watts is divided by the total number of racks that are planned for the space.

Which method is used is not as important as making sure that all comparisons between similar facilities use the same method. Usable UPS capacity is defined as how much of the actual UPS nameplate rating has

been designated in the design. Many owners and engineers designate 90% to 95% of the nameplate rating as usable UPS capacity as a best practice.

For data centers designed during the 1990s, 50W/ft^2 to 75W/ft^2 was common. In the 2000s, 150W/ft^2 to 200W/ft^2 is much more common. There are data centers that have been designed for significantly higher load density, 200W/ft^2, but that requires special cooling methods to remove sufficient heat from the IT equipment.

4.1.3 Single point of failure (SPOF)

A single point of failure is any one component, piece of equipment, or function that by failing causes the whole system to fail.

Consider the failure mode loss of fuel for an automobile. Most vehicles have only one fuel pump, so the fuel pump is a SPOF. If the fuel pump fails, the automobile stops. (There can be multiple failure modes causing the fuel pump to fail.)

Utility power can be a SPOF if there are no local generators. For facilities that have a local generator, as long as the utility power is available, the generator is not needed. Therefore, when a site has both utility power and a local generator, the generator is not a SPOF. (Protecting electronic equipment, which can only go 10 ms to 20 ms without power, generally requires a UPS system to provide power while the generator starts.) The local generator could be a SPOF only if there is no utility power (the generator is the only source of power for the site).

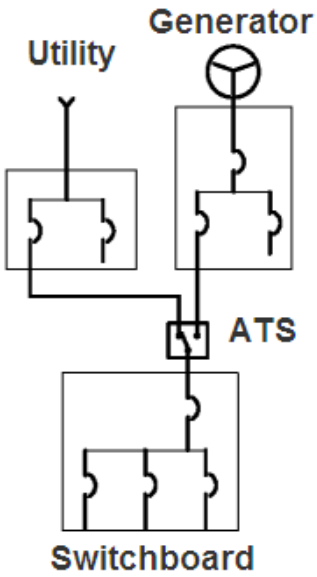

Figure 1—Basic electrical distribution system for critical loads

In Figure 1, the automatic transfer switch (ATS), the main circuit breaker, and the switchboard would all be SPOF, since the failure of any one of them would cause the loads fed by the switchboard to lose power. There are additional examples of SPOF for electrical distribution systems in 7.3.

4.2 Special electrical equipment to support continuous operation

There are several special pieces of equipment specifically designed to support the continuous power requirement of electronic equipment. The most common is a UPS, which is available in several types of technology. In the critical facility environment, the majority of UPS is double conversion, where ac power is converted to dc with a rectifier and then back to ac by an inverter. Some form of energy storage is applied to the dc bus to provide backup power in the event of loss of power to the rectifier. Batteries have long been used for backup storage, but some UPS suppliers offer other forms of energy storage, such as flywheels.

4.2.1 Uninterruptible power supplies (UPS)

There are UPS designs other than double conversion, such as standby (line interactive) and off-line. In a standby (line interactive) UPS, the inverter is operating but not carrying load unless utility power is lost. For an off-line UPS, the inverter does not start until the utility power is lost. There are also rotary UPS systems that employ synchronous generators instead of inverters for the output power.

Another very common piece of equipment is a static bypass switch (SBS). This is an electronic switch capable of shunting power around the UPS when UPS output voltage is outside of allowable tolerances. Many static bypass switches detect the loss of power and operate within a 1/4 cycle (25% of the period of the input voltage to the rectifier). They can be built into the UPS module itself or as a separate part in the control cabinet for multi-module UPS configurations.

In Figure 2, the static bypass switch is internal to the UPS module. Figure 14 shows a parallel redundant configuration of UPS modules with an external static bypass switch.

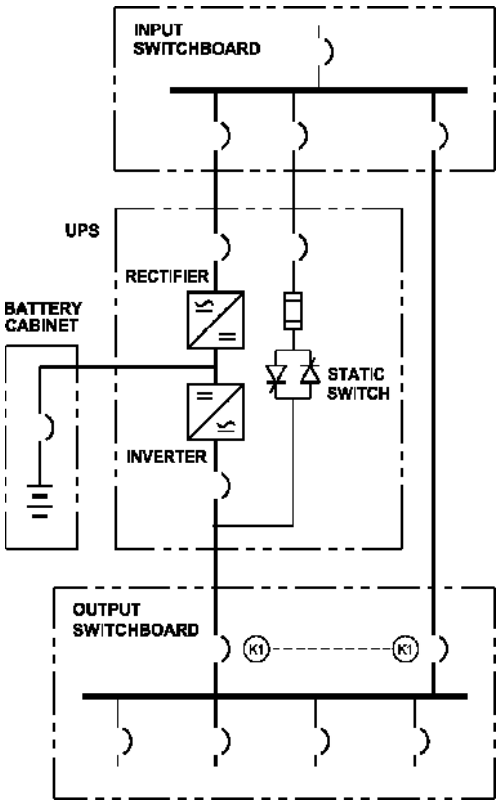

Figure 2—Double conversion UPS module with internal static bypass switch

4.2.2 Static transfer switches (STS)

In recent years, the same technology used for a static bypass switch has been applied to other transfer switches. An STS, shown in Figure 3, operates in a similar way to two static bypass switches supplying a common load. Typically, power is brought to each side of the STS from a different UPS. For a voltage deviation outside the specified limits on the primary side, it switches to the alternate, often within a 1/4 cycle.

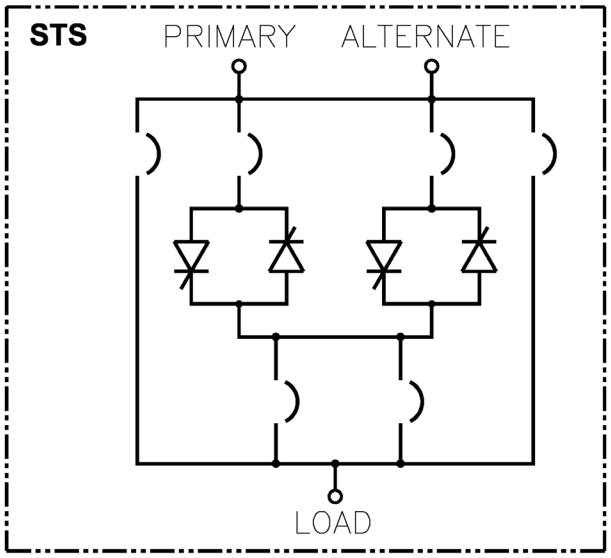

Figure 3 —Static transfer switch

There is a significant difference between the control of the static bypass switch and the static switch of an STS. The static bypass switch is triggered so that it makes (provides a closed transition) before the UPS inverter is shut down. The STS does the opposite. It opens one static switch as it transfers, then closes the other static switch (open transition). It is very important that the STS operate as an open transition, as a significant failure mode of an STS is a cross-connection in which both static switches are closed at the same time, thus both power sources are connected. This type of failure often causes both systems to shut down.

STSs can be relatively large, such as 4000 A, in which they supply power to multiple power distribution units (PDU). They are also made in smaller sizes to be mounted right on the rack with the information technology (IT) equipment itself.

The STS can also be used on the primary or secondary side of the PDU transformer. To install the STS on the secondary side, two transformers are required. Though it has a higher initial cost, it can provide benefit. The reason is it eliminates the problem of transformer inrush current during an out-of-phase transfer. The second transformer is already energized by the alternate source and therefore does not have to be reenergized while it still has a residual magnetic field from the first source (as it does in the case of a transformer with the STS on the primary side).

4.2.3 Power distribution units (PDU)

The PDU shown in Figure 4 consists of a transformer, distribution panel(s) with circuit breakers to supply the critical loads, and usually some form of built-in power monitoring. The transformer may be shielded, a K-factor transformer, or both. Some manufacturers of PDUs also provide surge protection in the unit.

Another common configuration is for the PDU to have a distribution panel that feeds remote power panels (RPP) or bus duct. Both RPPs and bus duct will have some form of overcurrent protection for the cables from the RPP or bus duct to the individual racks.

Some countries use 400 V/230 V or 415 V/240 V (and other similar voltage levels) for low voltage power distribution. For the majority of these systems, a transformer is not used between the UPS system and the IT loads. If a transformer is used, it is usually a 1-to-1 isolation transformer with shielding to prevent transients from reaching the IT load when the UPS system is in bypass.

4.2.4 Dual corded IT equipment

One of the most significant advances, from a reliability standpoint, is the development of dual corded IT equipment. Dual corded IT equipment has two power supplies built into it, with two separate power cords, each capable of powering the equipment, as shown in Figure 5. This provides the opportunity to eliminate SPOFs from the power source all the way to the piece of IT equipment itself. For many designs, the availability improves by a large factor in comparisons between single and dual corded equipment.

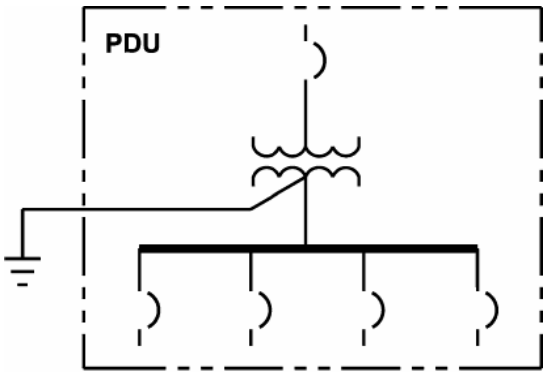

Figure 4—Power distribution unit

In order for dual cord equipment to improve availability and reliability, several conditions must be met. The equipment must provide notification when one of the power supplies fails. These notifications must be noted and repairs effected. Otherwise, the latent failure of the power supply will only be discovered when the power supply is needed and the equipment goes down.

It is also crucial to ensure that the cords are connected to different distribution systems that are not expected to fail at the same instant. Plugging the A and B cords into a circuit served from a single PDU is unlikely to improve the reliability and availability of the IT equipment.

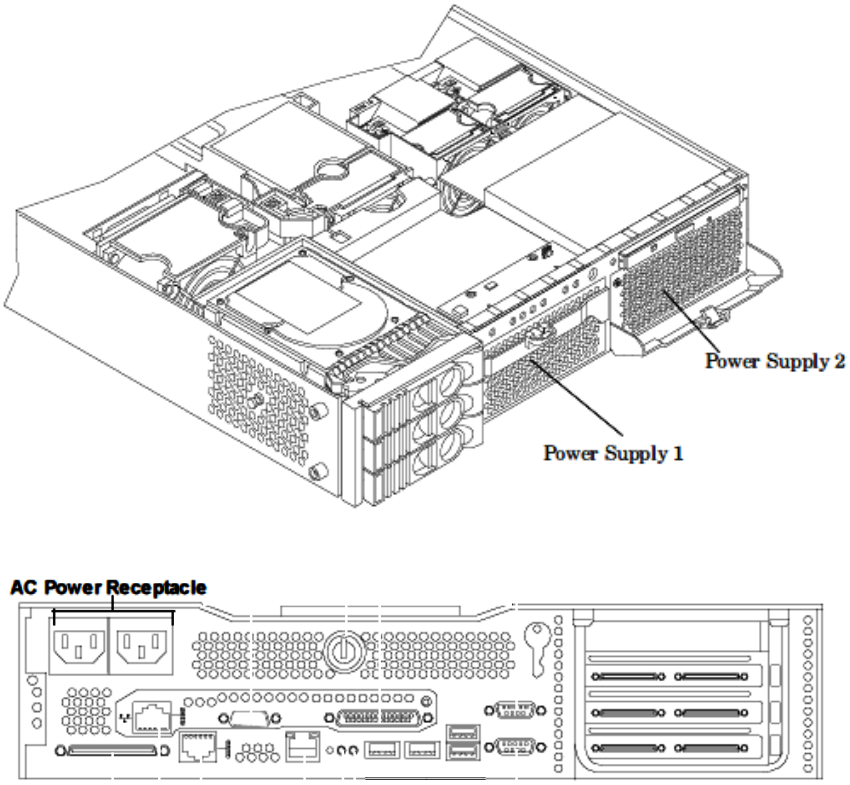

Figure 5—Dual cord IT equipment

Dual cord power supplies come in two basic types. One type utilizes regulated power supplies, where one side provides 95% of the power requirement and the other 5% is used to keep the second power supply energized. The other type uses unregulated power supplies with current sharing onto a common dc bus. The unregulated power supplies each provide 50% of the load current.

Some IT equipment designs use more than two power supplies, such as two-out-of-three or three-out-of-four designs. For these equipment designs, the manufacturer often provides an option that powers the multiple power supplies from two power cords with some form of internal switching.

A common configuration for chassis serving blade servers is to have six power supplies, three for each side fed phase-to-phase. For this type of equipment, the A side has a set of power supplies connected A-B, B-C, and C-A; and the B side also has a set of power supplies connected A-B, B-C, and C-A. The IT equipment can often be programmed to turn on the power supplies only as they are needed, which can cause considerable variation in the load on the UPS system.

The major factor that makes knowing how the various IT loads draw power important is maintaining the required capacity on both systems, so when one system fails and the load shifts to the other system, the remaining system does not overload. This is discussed further in 7.4.

4.3 Special mechanical equipment to support continuous operation

Momentary interruption of the electrical power is a significant failure the critical load must be protected from. UPS and standby generators are very common for a facility with IT loads considered critical. Special cooling equipment is also used when there is any significant amount of IT equipment, since most 7×24 facilities produce far more heat per room than typical commercial HVAC systems are designed to service.

The amount of energy consumed by the IT equipment in kilowatt hours is rejected into the computer room in the form of heat and must be removed in some manner.

4.3.1 Computer room air conditioning (CRAC) units

Computer room air conditioning (CRAC) units were first developed for mainframe computer rooms that required the temperature and humidity controlled within a specific tolerance. The CRAC unit, as shown in Figure 6, has a built-in refrigeration system and is often called CRAC DX, in which the DX is short for direct expansion. Direct expansion is a reference to how the unit creates cooling, by the expansion of the refrigerant. CRAC DX units use an air-cooled condenser, dry cooler, or cooling tower that is mounted outside the building to reject the heat. See 9.1 for typical systems using CRAC DX units.

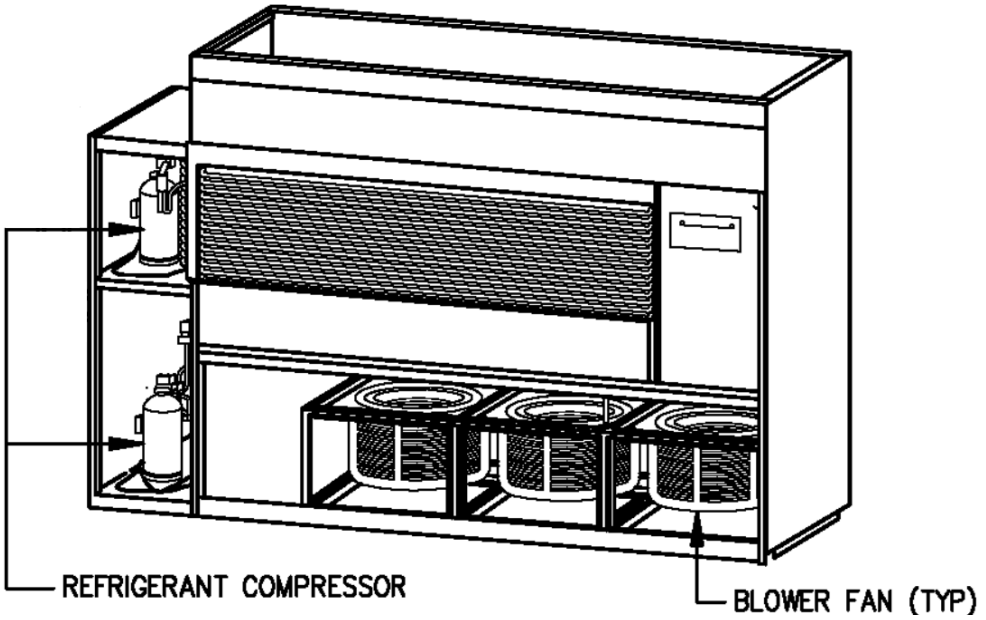

Figure 6—CRAC unit

4.3.2 Computer room air handling (CRAH) units

Where the refrigeration/air-conditioning equipment is not internal to the equipment, the units are often called computer room air handling (CRAH) units. CRAH units are similar to air handling units used for building air conditioning systems, only packaged to fit in the computer room. Figure 7 shows the CRAH unit, which has fans to pull the air through the cooling coil and push it out into the data center, usually under a raised floor which is used as a cold air plenum. CRAH units are used with water and air-cooled chillers, as shown in Figure 27 through Figure 30. The temperature in the data center room is controlled by how much chilled water is directed through the cooling coil by the chilled water control valve. Adjustable speed drives are often also used to control the blower fans, to increase the energy efficiency of the cooling system, and to provide a finer level of control for air flow through the data center.

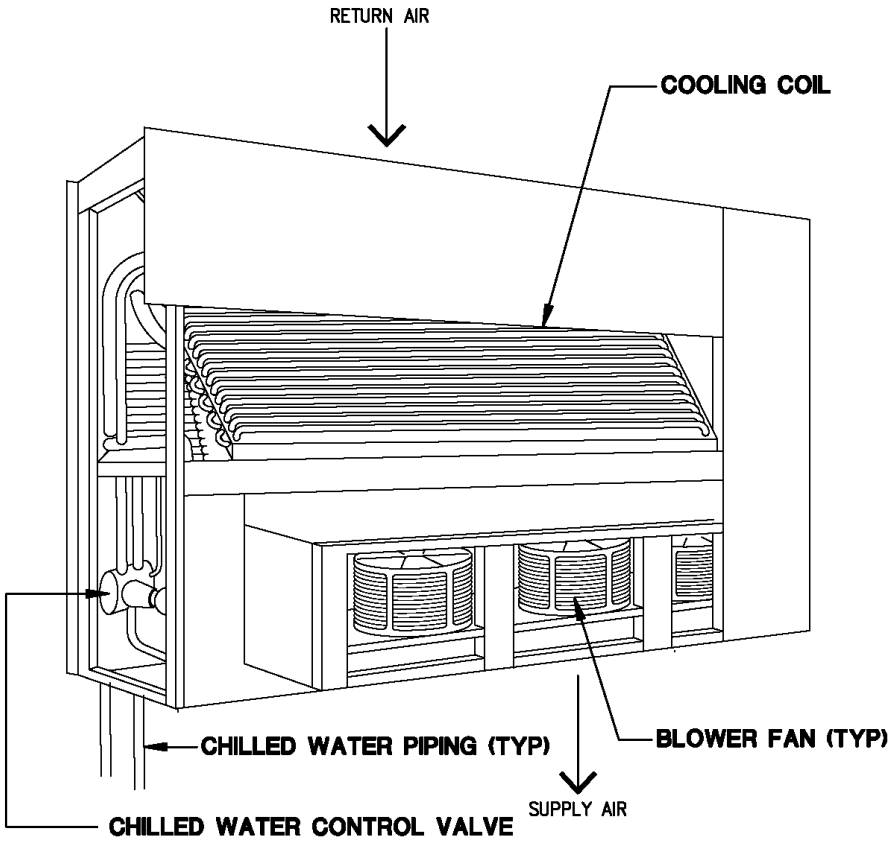

Figure 7—CRAH unit

5. Defining failure in a 7×24 facility

Calculating the reliability of a complex system requires a clear, unambiguous definition of failure. The definition of failure for a complex system can be complex. What constitutes a failure is often a function of which party requests the calculation of reliability.

Consider the case of a UPS module that fails but switches to internal bypass. The critical loads are not affected.

- The UPS vendor will consider this event a success because power to the critical load was not interrupted.
- The facility operations crew may consider this event a failure because it requires a significant effort on their part to organize and coordinate repairs to the failed UPS module.
- The business managers may consider this event a failure because the critical loads are exposed to utility voltage transients, which they consider unacceptable, and because they authorized the purchase of the UPS to prevent this occurrence.
- The users of the services performed by the critical loads are generally unaware of the UPS module failure. Since they are not affected, they might consider this event a success.

Another significant issue is what constitutes a failure at the individual critical load itself, usually some piece of computer or IT equipment. In a large data center there will be thousands of individual loads. There is usually redundancy for the computers or other IT equipment, and they often work in conjunction with each other. A majority of the time the interactions are so complex that it is not possible to determine with any degree of accuracy exactly which of the machines will take care of a specific application or data

communication. Should the loss of one load constitute a failure? It may have no impact whatsoever to the overall mission of the facility.

Another aspect of this same issue is that in most critical facilities, there are multiple PDUs or UPS distribution panels in the facility. In each panel there are multiple branch circuits. If a failure was defined as the loss of an individual circuit, several factors would immediately be apparent. First of all, the type of system upstream of the panel would be relatively insignificant in the calculations compared to the number and failure rate of the individual branch circuits. Secondly, the bigger the data center, the worse the availability and reliability would be regardless of the design. Therefore, it does not make sense to go to the individual branch circuit level as it skews the results based on size.

The effect of the size of the facility on the reliability and availability of the data center will be discussed in more detail in 8.2.

A third aspect of defining failure is establishing what the data is to be used for. There is no point in collecting vast quantities of data that is insignificant and obscures data that is significant. So it may be easier to reverse engineer the definition of failure by looking at what would be significant data.

Clause 5 recommends definitions for failure of the various components, systems, and subsystems in a 7×24 facility. Subsequent clauses will discuss why these particular definitions were selected and recommend what failure data to capture for the various components and subsystems.

5.1 Failure of components

The following are considered component failures:

Automatic static transfer switch—Failure to transfer or loss of power at the load terminals for any reason except no input power to either side of the switch.

Automatic transfer switches (mechanical)—Failure to transfer or loss of power at the load terminals for any reason except no input power to both inputs of the switch.

UPS battery—Loss of power to the inverter it is supplying, whether due to discharge, connections, or internal cell failure.

Chiller—Less than rated cooling provided when required. (Unit may cycle on and off, based on load. Therefore only if it failed to cycle on and provide cooling when required would it be a failure of the unit.)

Circuit breaker—Loss of power to the load it is feeding, regardless of where in the system it is located, except when a fault in the cables or equipment it is feeding caused the circuit breaker to open. It would also be a failure if the circuit breaker closed when it was not supposed to due to a defective control or part. A primary function of the circuit breaker is also to detect overload, short circuit, or ground fault conditions, so it would also be a failure (often latent) of the circuit breaker if it failed to properly detect these conditions.

CRAC or CRAH unit—Less than rated cooling provided when required. (Unit may cycle on and off, based on load. Therefore, only if it failed to cycle on and provide cooling when required would it be a failure of the unit.)

Fused switch—Loss of power to the load it is feeding, regardless of where in the system it is located, except when an overload or short circuit in the cables or equipment it is feeding caused the fuse to open.

Generator—No output power, voltage, and/or frequency out of tolerance, when required.

NOTE—It is important to capture whether the generator failed to start, or whether it failed while operating, as will be discussed in more detail later in this document.[4]

Pumps—Less than rated water pressure or flow, provided an adequate supply of water at the proper input pressure is available to the pump.

Static bypass switch (for UPS module)—Failure to transfer or loss of power at the output terminals for any reason except no input power to input of the switch (when called upon to be operated by either UPS module failure or manual switching operation).

UPS module rectifier—Failure to provide power at the dc bus, regardless of whether the battery is charged and providing power to the inverter, except when power at the input of the rectifier is out of tolerance due to a failure upstream.

UPS module inverter—Loss of output power at the inverter in any failure mode except for loss of dc input (which is a battery or rectifier failure, not a UPS inverter failure).

NOTE—Whether or not a static bypass switch operates is inconsequential to the UPS module failure, though it would be very significant at the subsystem level.

5.2 Failure of the subsystem

The following are considered subsystem failures:

UPS system (UPS module with static bypass switch for single or multi-module system)—Loss of power to the load it is feeding, including momentary sags where the voltage disturbance is outside the specified limits, as the purpose of the UPS module was to protect against this in the first place. Therefore, it is a failure of the subsystem if there is a voltage disturbance outside the specified limits while the load is on the static bypass switch.

Mechanical cooling subsystem for the critical load—Less than the number of cooling components required (or available) for the subsystem. For example, a chilled water plant consists of three cooling systems, each one consisting of a dedicated cooling tower, condenser water pump, chiller, and primary chilled water pump. If any one of these five components (cooling tower, condenser water pump, chiller, or primary chilled water pump) fails, that subsystem will not be available to provide cooling.

5.3 Failure of the critical electrical distribution system

The definition of failure for the critical electrical distribution system depends on how the mission has been defined. Service level agreements (SLA) are often used to define the specific mission of the facility.

Basically, failure is anything that prevents the mission from being accomplished. The following are examples of typical definitions for failure for critical electrical distribution systems:

- Loss of power for a single rack
- Loss of power to a UPS panel
- The loss of power to a PDU

[4] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

— Loss of UPS system power

If the facility has dual cord loads fed by two different panels, PDUs, etc., a failure would be the loss of power to both panels or PDUs. This will be discussed in more detail in the following subclauses.

5.4 Failure of the critical mechanical cooling system

Failure of the critical mechanical cooling system is defined as loss of the required cooling capacity, regardless of what part of the cooling system has less than the required number of components operational. For example, if there are nine CRAC units and seven are required to provide adequate cooling for the data center room, it would be a failure any time there were less than seven CRAC units operating (or available).

For the example of a chilled water plant that consists of three cooling systems, each one consisting of a dedicated cooling tower, condenser water pump, chiller, and primary chilled water pump, if two out of the three systems could provide the required cooling, any time less than two complete systems were available it would be a failure of the mechanical cooling system. For this example (since the cooling towers and pumps are all dedicated to a specific chiller), if a condenser water pump on one system failed at the same time a primary chilled water pump on one of the other two systems failed, that would be a failure of the mechanical cooling system.

Failure of the critical mechanical cooling system is significantly different than failure in the critical electrical distribution system. When power is lost to the critical load on the raised floor, there is an immediate failure. However, when the cooling is lost, it may take a certain amount of time for the temperature to build up and cause the critical load to overheat and shut down. In low density applications, it often takes at least several minutes (and sometimes much longer) for the temperature to build up to an unacceptable level. (In high density applications where the temperature builds up to unacceptable levels in a couple of minutes or less, there are usually UPS systems to provide power to the CRAH units and the secondary chilled water pumps.)

The reliability models for the mechanical cooling system required to take into account this residual cooling in the system would be extremely complex. Not only do different types of IT equipment have different cooling requirements, the cooling across the room itself is not completely uniform for all of the racks, all the locations in the racks, etc. Therefore, the usual method of analysis for the mechanical cooling system is determining the probability of the cooling system being lost, not the probability that the critical load will actually shut down due to overheating. The reliability calculations for the mechanical system may be more conservative than what actually occurs in data center operation.

There is another important aspect for the modeling of the mechanical cooling system that is different from modeling the electrical power to the critical loads. For the electrical power to the critical loads, the power is always required to the whole critical distribution system. The load on the IT equipment itself may vary with usage, but the power is always required to all of it. For the mechanical cooling system, the cooling load significantly varies in even a 24 h period and in many places varies dramatically throughout the year. On a design day (the most demanding ambient environment the mechanical system is designed to provide cooling for), the whole mechanical cooling system may be only N+1. But 50% of the year the whole mechanical cooling system may be N+2 (or have even more redundancy). The reliability models are not capable of accounting for this variation. The reliability model normally assumes the cooling system is operating under peak load of a design day 24 h a day for the entire period being modeled.

5.5 Failure of the electrical power to the critical mechanical cooling system

The definition of failure for the electrical power to the critical mechanical cooling is loss of power to any or all of the required equipment. For this definition, required equipment includes just the required number of

components (N) for the entire mechanical cooling system, regardless of whether or not the redundant components also have power. For a chilled water central plant (see Clause 9), the required equipment would include the required number of cooling towers, condenser water pumps, chillers, primary water pumps, secondary water pumps, and CRAH units to carry the peak cooling load.

For this definition, loss of power is based on the basis of design for the system. If the basis of design is that the chilled water plant shuts down on loss of utility power and restarts when the generators come up and restore power, momentary outages would not be considered a failure. Only prolonged outages, such as when the generators failed to start or transfer, would be considered a failure. (This is the most common basis of design for chilled water central plants.)

With the development of blade servers, the amount of heat to be dissipated from each rack has dramatically increased. The time delay between the loss of the mechanical cooling systems and the overheating of the IT equipment has been greatly reduced. In a modern data center designed for blade servers with a density of 200 W/ft^2 or greater, some of the cooling equipment (such as the CRAH units and secondary chilled water pumps) are often on UPS power to provide some continuous cooling while the rest of the chilled water plant restarts. For mechanical cooling systems on UPS power, any loss of power (even a momentary one) would be considered a failure since the UPS system was design to provide continuous power to that equipment.

5.6 Other types of failure

Quite often a failure in the critical facility is the result of failed equipment. But there are other types of failure that must be considered, such as an incomplete or incorrect design. An example would be an electrical system in which a short-circuit in one critical branch circuit cascades several levels of overcurrent protective devices, unnecessarily taking out of service an entire UPS distribution panel, entire PDU, or worse, the upstream feeder or even main overcurrent protective devices. This type of error is often the result of an incomplete coordination study, which has not evaluated all of the possible configurations of the distribution system. There are two common examples in which the available fault current changes significantly from the normal configuration. The first is when the UPS system is in maintenance bypass, or the static bypass switch turns on. The available short-circuit current to the UPS output switchboard is much greater on bypass than when the UPS modules are providing power. The second situation is when the facility switches from utility to generator power. In the vast majority of the cases, there is much less available fault current on generator power than on utility power. The reader is encouraged to refer to the IEEE 3004 series of recommended practices covering the selective coordination of overcurrent protective devices for more information.

6. Reliability and availability as tools in evaluation of critical facilities

When evaluating the reliability of a system, the general rule is the fewer components there are that are required to operate the system, the more reliable it will be. This was probably first discovered in terms of moving parts for mechanical equipment. The more moving parts the piece of equipment has, the more opportunities there are that something will fail. In terms of the reliability analysis, each component can be considered a link in the overall reliability chain.

Another general rule is that the reliability is improved by the elimination of SPOFs. Each link of the reliability chain is an SPOF. Any one link can break and cause the chain to fail. However, if there are two chains, each one fully capable of carrying the load individually, all the SPOFs would be eliminated, dramatically raising the reliability of the overall system. This is also referred to as providing redundancy. The second chain is redundant.

Another aspect of eliminating SPOFs with redundancy is to eliminate the common mode events that could bring down both systems. A typical example is a redundant UPS module where the controls, output bus, output breaker, or the static bypass switch are common devices. A failure in one of the common devices can bring down the entire system in spite of the redundant UPS module.

6.1 Reliability and availability—importance of using both

From looking at the definitions of reliability and availability in 3.1, there are some important differences between these two concepts. Reliability is time dependent. The longer the time, the lower the reliability, regardless of what the system design is. Availability is more or less independent of time since it is the ratio of two means (averages). In the case of inherent availability (Ai), it is the mean time between failures (MTBF) divided by [MTBF + mean time to repair (MTTR)]. This encourages the use of availability when comparing system designs and looking for an index of quality. Hence, terms such as "5-9s" (meaning an Ai of 0.99999) have become common.

Availability can be a prediction of future performance or a measure of past success. In the case of past success, achieved availability is the percentage of time the system was operating. An availability of 0.99999 would mean that the system was down for 5.3 min, or 315 s, per year. It would make no difference in the availability calculation if there was one 5.3 min outage or 315-1 s outages. It could also be one outage of 1.77 h in 20 years. In all three cases, the availability is 0.99999.

To the operation of electronic equipment in a critical facility, there are huge differences between the three cases described, which is why reliability is also an important index. In the example of 315-1 s outages, the reliability for a one week period would be zero, since there is an average of 26 failures a month. For the example of one 5.3 min outage once a year, the reliability would be significantly better, but still probably unacceptable for most critical facilities. However, for most critical facilities, a single outage of 1.77 h in a 20-year period would be an acceptable performance.

This discussion shows that availability by itself does not completely address how often a failure occurs. It is just a combination of how often it fails and how quickly it is repaired. Critical facilities require both high availability and high reliability.

In a utility distribution system, particularly in areas with overhead distribution lines, a high availability can often be achieved using reclosers. A very common scenario throughout the mid-western part of the U.S. is that a tree branch is blown into the power line during a storm. The recloser opens to clear the initial fault, then immediately recloses. The initial fault blew the tree branch to pieces, so the recloser restored the power. The total outage time could be a few seconds or less, and therefore the availability could be quite high. However, all the customers on the line downstream of the recloser would have experienced a momentary outage (and have to reset their electronic clocks).

With computer and other IT equipment, repairing the failure by getting power back does not restore the data that was being processed. Data is lost, the programs may be corrupted, or the machine may not be successful in the rebooting process and require additional operator intervention. The explosive growth of the UPS industry paralleling the computer industry is testament to how important it is to provide continuous power and avoid even very short outages of a few cycles.

6.2 Reliability and availability as tools in design evaluation vs. evaluation of a specific facility

One of the most successful uses of reliability engineering is in evaluating and improving equipment design. Calculations can be performed for the component level, such as a UPS module, to improve its design. They

can also be done as a comparative tool to evaluate how best to configure subsystems, such as multiple UPS modules. In each case, the purpose of the calculation impacts how the model is developed.

As mentioned earlier, the purpose of doing reliability analysis can be defeated by improperly modeling the equipment or system (e.g., modeling every PDU in a large facility and comparing it to a small facility with only a couple of PDUs). The small facility will have better reliability and availability numbers, just because there are fewer PDUs to fail. The large facility may actually have a much better design configuration with built-in redundancy, but appear to be much worse. In this case, a better comparison of the design for the two facilities would probably be gained by using only a few of the PDUs with the large facility.

Another significant factor that can utterly defeat the purpose is incorrect failure rate data. The best data would be the actual failure data of the facility. However, this is often not available, and published failure rate data is the best source of information. The published failure rate data for most of the electrical power equipment in this book is probably somewhat conservative for 7×24 facilities since it comes from a broad cross section of facilities. Most 7×24 facilities have a much cleaner and more controlled environment than the average facility, particularly when compared to industrial sites.

However, the real issue with failure rates for a 7×24 facility is the shortage of statistically valid data for special equipment, such as UPS modules, STSs, etc. A significant portion of the published data that is available comes from the manufacturer of the equipment. The obvious conflict of interest to show their equipment in its best possible light makes this source of information suspect. It is not uncommon for different manufacturers to use different failure criteria; they each define failure such that their equipment is superior to that of their competition for equipment failure rates. The subclause earlier in this recommended practice defining failure for components and subsystems is an effort to at least standardize this aspect of the data collection.

A third factor that is an inherent limitation of any type of modeling is that someone has to make qualitative judgments as to what is significant and what is not. Therefore, reliability models that compare one design to a similar design are usually of more value than models that try to predict the reliability and availability of a specific system. It is important to develop an operational profile or theory of operation for the system that includes the definition of failure, what happens in the event of a failure, and degradation of the system during operation, etc., and get buy-in for this profile from the owner.

As a comparative tool to analyze two similar designs, it is much easier to minimize the effects of these factors on the accuracy of reliability analysis. For example, the failure rates used in the calculations may be significantly higher or lower than the actual failure rates for a specific facility. Therefore the availability and reliability calculated would also be higher or lower than they really should be. However, when comparing two designs, the same failure rates would be used for both designs. Therefore, the difference in availability and reliability for the two designs would be unchanged by the fact the actual failure rates for the facility were either higher or lower than what was used for the calculations.

6.3 Recommended reliability tools for evaluation of 7×24 facilities

There are several modeling techniques in reliability engineering that are suitable for performing reliability analysis on the electrical and mechanical systems in 7×24 facilities.

6.3.1 Reliability block diagram

Reliability block diagram (RBD) is a block diagram in which the major components are connected in the same manner as they are in the one-line, or piping, diagram. From left to right in Figure 8, the blocks are utility power, two fused disconnect switches, two transformers, two circuit breakers, and a main switchgear. Each of the blocks have the failure and repair data for that component included in the block. The junctions connecting the block are set to account for the system redundancy (e.g., one out of two as

shown in Figure 8 between the circuit breakers and the main switchgear in which there are two components in parallel and only one is required to carry the load). Quantitative results (reliability, availability, MTBF, etc.) for the RBD are obtained by performing the series and parallel combinations, etc. of the blocks.

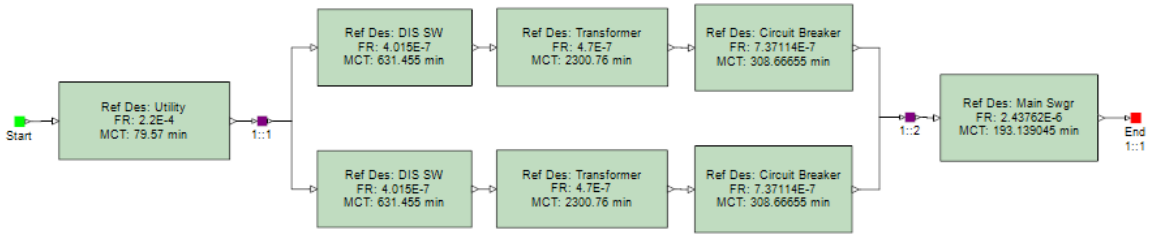

Figure 8—RBD of utility power to two transformers, either one of which can power the main switchgear

RBD is an excellent method to model systems such as the critical electrical distribution and the mechanical cooling systems. The RBD models the one-line, or piping, diagram to be analyzed, which makes this methodology more understandable to engineers without much background in reliability engineering.

6.3.2 Fault tree analysis

Another modeling technique of reliability engineering that is very useful for 7×24 facilities is fault tree analysis (FTA). FTA is a systematic, deductive methodology for determining all of the credible ways for a specific undesirable event to occur. The undesirable event to be analyzed is the top event of the fault tree. The fault tree uses Boolean algebra (AND gates, OR gates, etc.) in a graphical representation to show the logical interrelationships between the initiating basic events, such as component failures, environmental factors, or human errors, etc. that can ultimately lead to the undesirable (top) event. Quantitative results (reliability, availability, MTBF, etc.) for the FTA can be obtained if failure data is available for all of the initiating basic events in the fault tree.

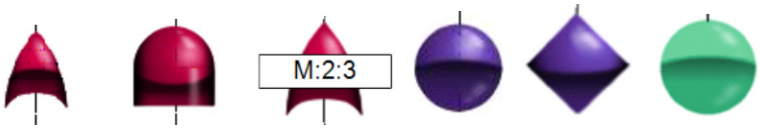

Figure 9—Fault tree symbols: OR, AND, voting gate, initiating (basic) event, undeveloped event, and repeated event

The OR gate has an output if any of the inputs are true. The AND gate has an output if all of the inputs are true. The voting gate has to have the number specified out of the total number true to have an output (in Figure 9, it requires two out of three to be true).

Undeveloped events are points where the FTA was stopped, but it could be taken further. For the FTA, they function the same as a basic event. Repeated events are the same as basic events, but they appear in more than one place in the fault tree. An example fault tree is shown in Figure 10.

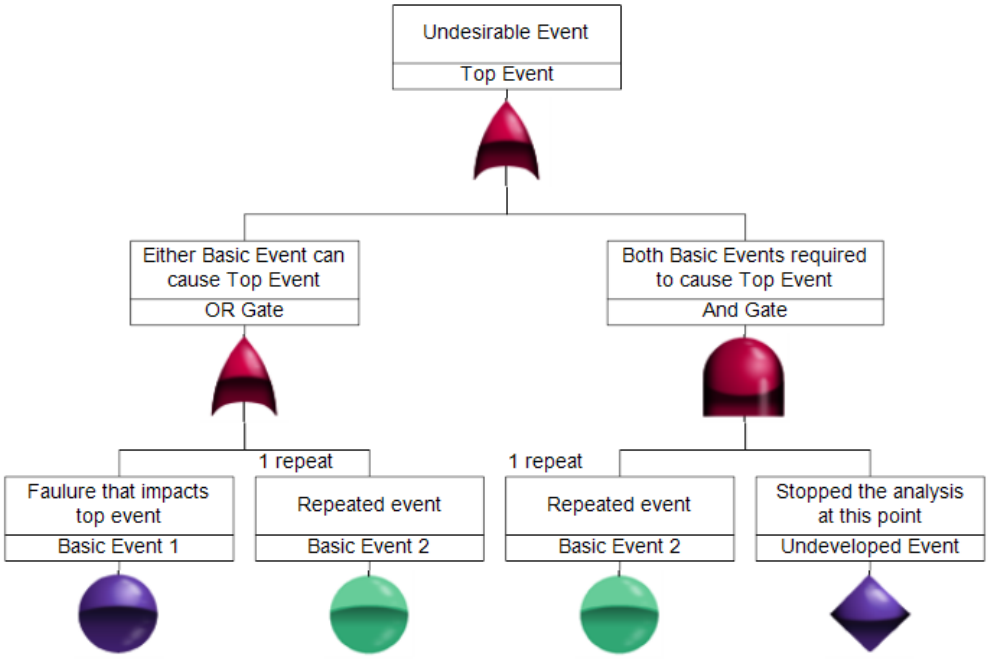

Figure 10—Example fault tree

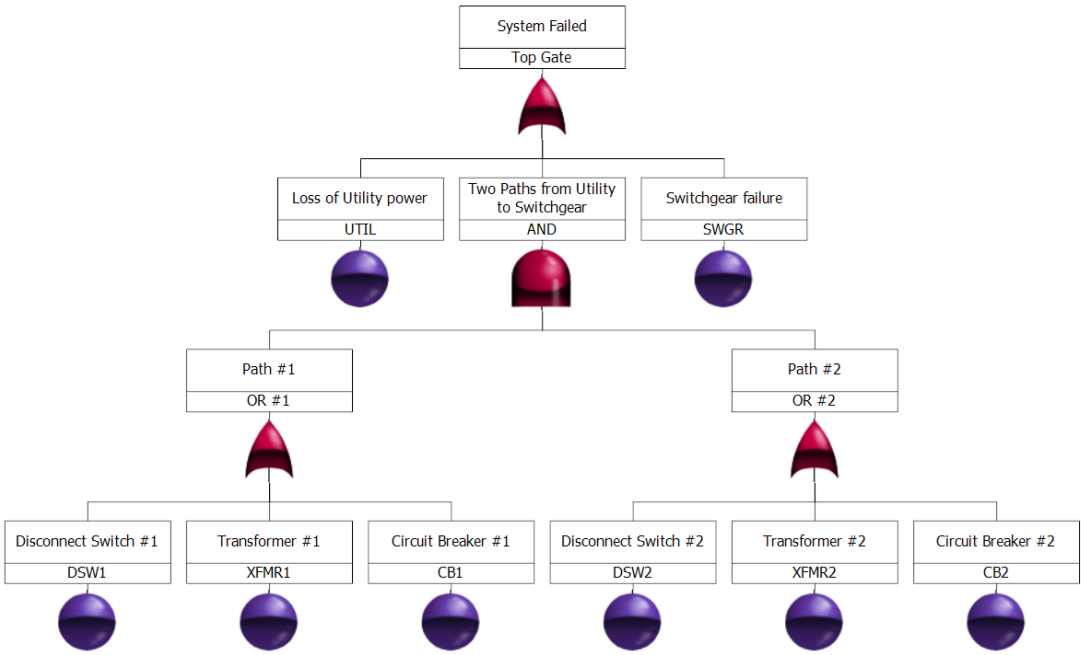

Figure 11—Fault tree of the same system shown in Figure 8

6.3.3 Failure mode effects and criticality analysis

Failure mode effects and criticality analysis (FMECA) is also a very powerful tool in reliability analysis. It is often referred to as a FMEA with a criticality analysis.

In a FMECA, each element in a system is examined individually and collectively to determine the effect when one or more elements fail. This is a bottom-up approach: each of the elements is examined, all of the ways it can fail are listed (failure modes), and the effect of each failure to the element itself and on the overall system is predicted.

IEEE Std 3007.2-2010 has a detailed example of a FMEA for a 480 V switchboard that demonstrates this process.

Once all the failure modes and effects have been defined, the next step is to look at the criticality of the effects in conjunction with the probability of each one happening. The normal method is to have a gradient scale of criticality such as:

I. Catastrophic (major human injury, significant financial loss, significant PR impact)
II. Critical (significant loss of production, minor human injury)
III. Marginal (minor loss of production)
IV. Minor (no impact to production that is significant)

The probability of each failure is then addressed. Another gradient scale is often used, such as:

A. Frequent
B. Reasonably probable
C. Occasional occurrence
D. Remote
E. Extremely unlikely

Then each failure and its associated effect is evaluated in terms of the above two scales of criticality and likelihood of occurrence and put into a matrix as shown in Figure 11.

If the system has been very well designed, there will be no catastrophic events that are likely to occur. The FMECA matrix points out which areas need to be addressed that will give the greatest impact to the overall operation of the system. It also shows which areas not to bother with, as they are either extremely unlikely to occur or the effect when they do occur is minor.

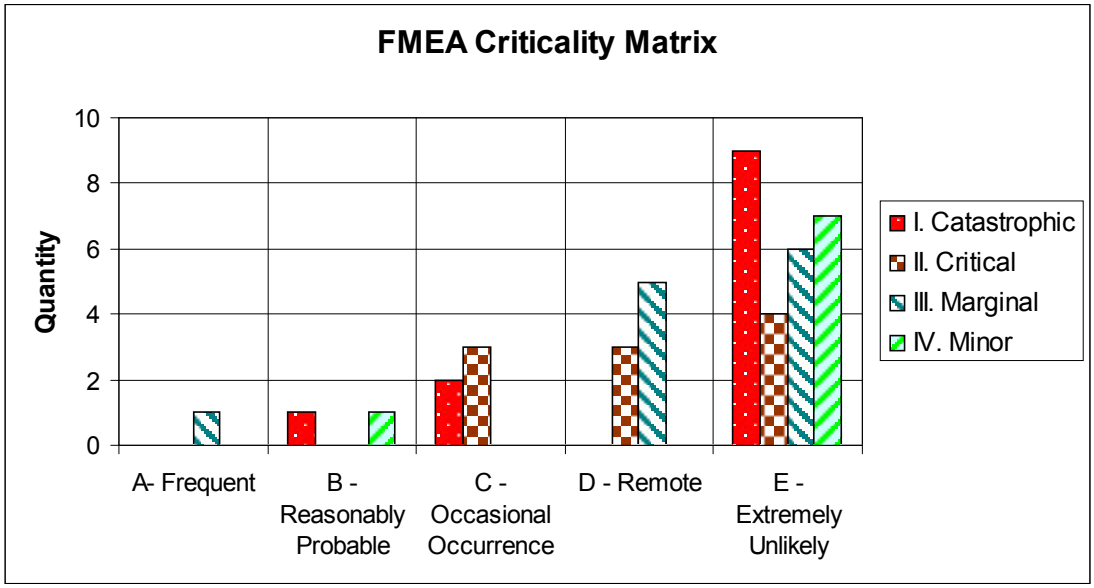

Figure 12—Example FMEA criticality matrix

6.3.4 Using RBD to model 7x24 facilities

IEEE Std 493™ (*IEEE Gold Book™*) provides the equations to perform simple series and parallel combinations of an RBD to determine availability and reliability respectively. For a quick comparison of simple systems or to get some idea of the impact adding redundant components would provide, a simple series/parallel calculation can be useful. However, 7×24 facilities are seldom simple systems, and the oversimplifications required to use series/parallel calculations can provide skewed results from what a more comprehensive analysis would provide.

The major factor in 7×24 facilities that makes series/parallel calculations inadequate is standby equipment, such as standby generators, UPS batteries, and the static bypass switches which are part of the UPS system. The series/parallel calculation has to assume they are always available when needed.

If battery charge is not included in the analysis, it would not matter whether or not the standby generator started since the battery will last for as long as it is needed. These two items (battery running out of charge and the generator not starting) are precisely the items that are most likely to cause a real data center to fail!

Therefore, to properly model a 7×24 facility, reliability software that can address standby equipment is needed. The software uses what is called a Monte Carlo simulation to analyze an RBD that has standby equipment and repairable parts.

A simple explanation of how the Monte Carlo simulation is used to calculate the reliability of RBD is that it runs many (e.g., 10 000) simulations. For each simulation, a random set of blocks in the RBD are failed based on the failure and repair rates of the individual blocks. The software then performs an analysis on the remaining blocks in the RBD to determine if the RBD has passed or failed. (If the RBD has a complete path with the required number of units operating between start and end, the RBD has passed.) After it has run all of the simulations, it averages all of the results for each simulation and provides the availability, MTBF, and reliability of the RBD.

RBD directly models the flow of the electrical or mechanical cooling system. It may or may not address common cause failures (a failure that impacts multiple pieces of equipment or multiple systems), depending on the failure and how the modeling is done. It normally does not address factors such as manual switching by an operator in the analysis.

6.3.5 Using FTA to model 7×24 facilities

As described above, FTA follows a logical sequence in determining all of the feasible causes of an undesirable top event. It is a very powerful tool that can include the impact of various factors between systems, common cause failures, and even to some extent human failures.

A word of caution is in order to the novice in FTA. It is a tool that requires an in-depth understanding of the equipment and systems being modeled. The very power of FTA (being a logical sequence in determining all of the feasible causes) can also be its biggest weakness—the burden of determining ALL of the feasible causes is on the one developing the fault tree. Unlike modeling with RBD, in which just following the one-line will provide a model with all of the equipment in the system and how it is connected, developing a comprehensive fault tree may not be as intuitive.

FTA is an excellent tool to analyze specific failures that have critical importance to the 7×24 facility. By working backward from the failure to be prevented down to all of the items that could cause this particular failure, interfaces between equipment and systems can be brought to light that may be overlooked with other types of analysis.

FTA can also be a very effective reliability tool for qualitative analysis with items such as human errors that cannot be easily quantified with failure and repair rates. For example, a fault tree can be used to show the interrelationship between the automatic and manual controls on a mechanical cooling system.

7. Critical electrical distribution system configurations

7.1 Common configurations of the UPS system

Momentary interruptions of the utility power are a very significant failure from which the critical load must be protected. The voltage tolerance curve developed by the Information Technology Industry Council, usually referred to as the ITIC curve, is used by most manufacturers to define what acceptable power is considered to be. Any voltage outside the tolerance curve would impact the operation of the IT equipment, so UPS systems were developed to prevent this type of failure.

The simplest and most common UPS configuration is a single module with an internal static bypass switch. The critical load is protected from the momentary interruptions, along with complete outages by the energy stored, usually in batteries. If the UPS module fails, the static bypass switch transfers the critical load back onto utility power.

When the inverter of a single module UPS fails, the static bypass switch transfers the load to utility power. This exposes the critical load to momentary sags, which is what the UPS was installed to protect against in the first place. This led to the isolated redundant configuration shown in Figure 12. In an isolated redundant UPS, the inverter of a second UPS module feeds the static bypass switch of the first module. Therefore, the static bypass switch transfers the critical load to a second UPS module instead of utility power.

A primary disadvantage of the isolated redundant configuration is the step loading of the second UPS module. The redundant module goes from no load while the first module is in operation, to full load in a single step. This type of operation is difficult for a static UPS module to respond to and maintain the voltage within specified limits. Another disadvantage is that a fault on the output of the UPS module cascades from the first to the second UPS module, which can be a concern if there are separate power sources for the two UPS modules.

Shown in Figure 13, the parallel operation with a single static bypass switch was developed as a better configuration for utilization of the UPS modules. In parallel operation, two (or more) UPS modules operate in parallel sharing the load. Redundancy can be built into the design such that if one of the modules fails, the remaining modules pick up the additional load. In the case of two identical UPS modules, each operates at half of its full-load rating; the step load is now half what an isolated redundant configuration would experience. For three identical UPS modules, with one as redundant, each module would carry 2/3 of full load, until one module failed. Then the remaining two would each pick up 1/3 of full load in a single step.

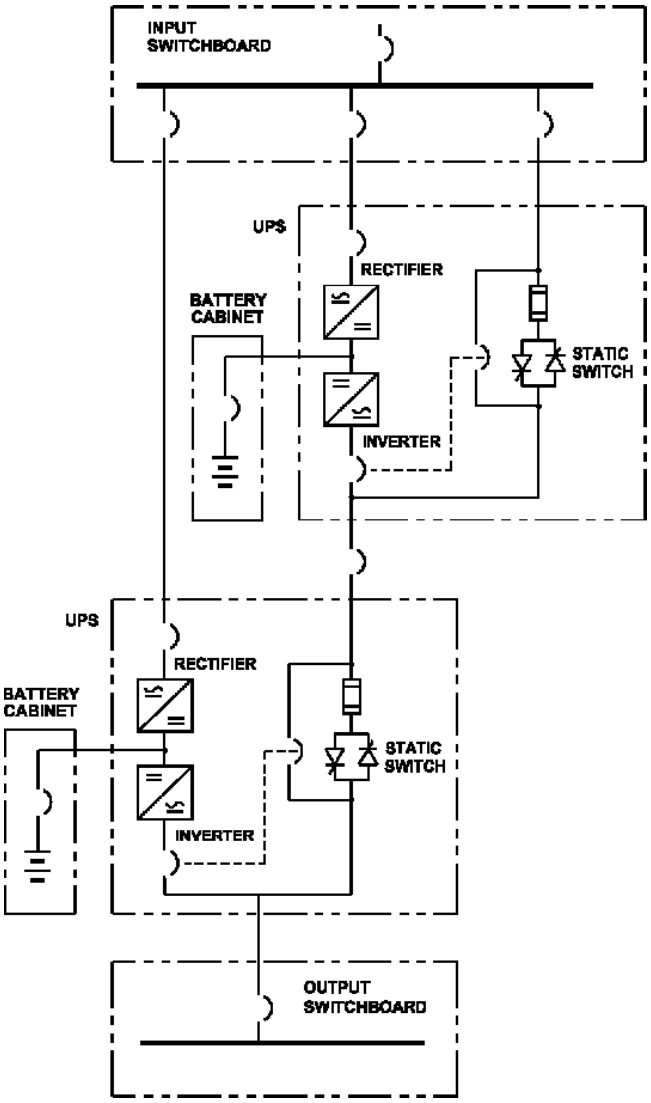

Figure 13—Isolated redundant UPS system

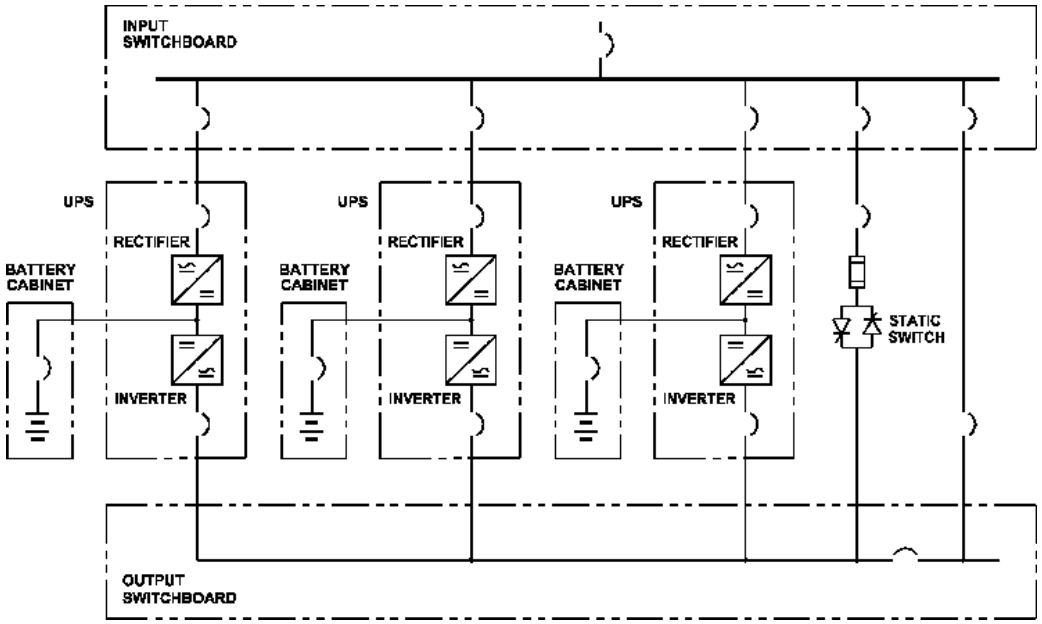

Figure 14—Parallel operation—Three UPS modules with a system static bypass switch and maintenance bypass circuit breakers

These examples of three UPS modules in parallel operation have a second advantage. Each module operates at 2/3 of full-load rating, instead of 1/2. This is more efficient in terms of both energy usage and utilization of resources. However, a parallel redundant system requiring one out of two UPS modules will be more reliable than a similar system that requires two out of three UPS modules.

The main disadvantage of the parallel operation is the presence of several SPOFs. The input and output switchboards are both SPOF, along with the static bypass switch and the system controls. A common example of the output as a SPOF is for an internal failure of a UPS module. This could result in the loss of the entire system should the circuit breakers and UPS controls fail to isolate it quickly enough. A typical scenario starts with an output filter capacitor shorting. The remaining UPS modules feed the fault, and the output voltage begins to collapse. The UPS system controls sense the collapse in output voltage and turn on the static bypass switch, directly feeding the fault from the utility source. If the magnitude of the fault current is high enough to trip the breaker feeding the static bypass switch (or the ground fault on the main circuit breaker feeding the input switchboard), power is lost to the critical load.

To eliminate the SPOF, multiple systems are needed. This will be discussed in more detail in subsequent subclauses.

7.2 Critical electrical distribution system designs

A common aspect of many critical distribution systems is redundancy; there are more key components than are necessary to carry the total load. The two most common key components to have redundancy are the UPS modules and the emergency generators.

When discussing redundancy of a system, it is common to refer to what is required as N (for number). If a facility has two standby generators and both are required to carry the building load during a power outage, N is two. If a third generator is added, the redundancy of the power generating system will become N+1. There would also be 50% redundancy in standby generator power.

If the facility has two standby generators and only one is required, the redundancy would also be called N+1. This could also be called 2N to show there is 100% redundancy in standby generator power. It

depends on how the generators are configured to determine which term is preferred. If the generators are in parallel, it would be N+1. If there are two systems totally independent of one another, the redundancy is 2N.

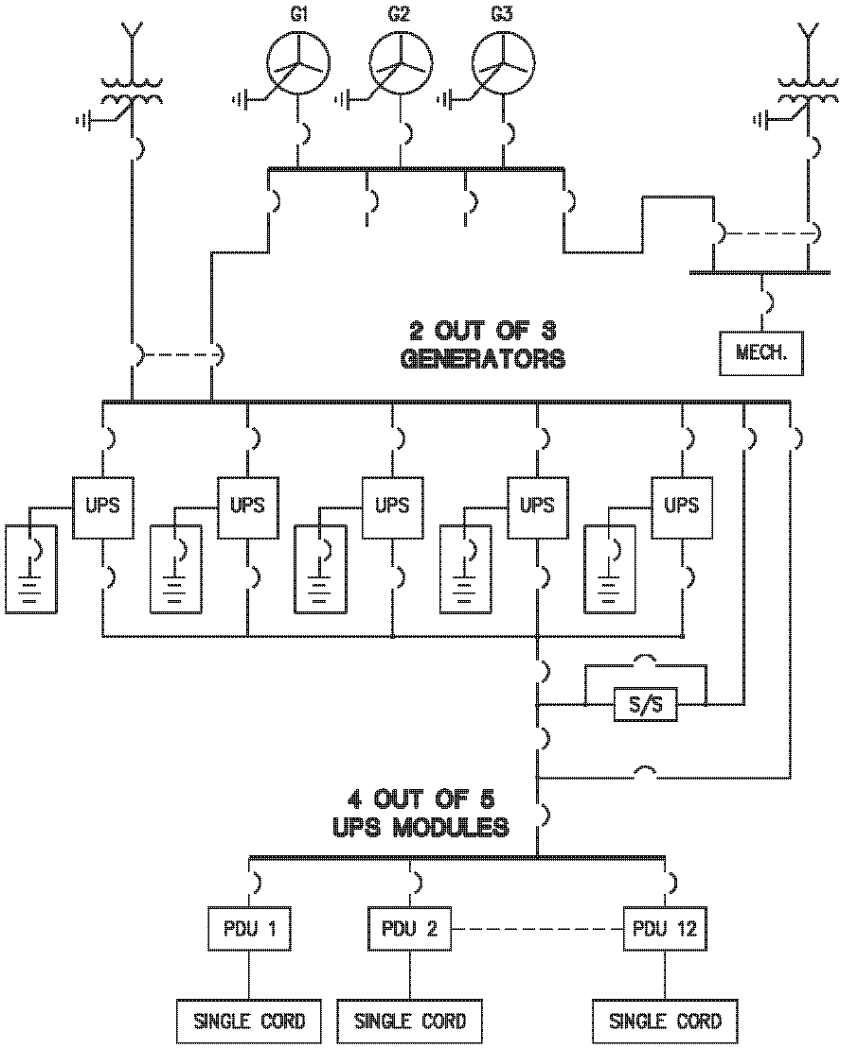

Figure 15—N + 1 generators and UPS modules

Shown in Figure 14 are three generators that connect to a generator-paralleling switchboard providing backup power to a critical distribution system. There are five UPS modules connected in a parallel redundant configuration with a static bypass switch in a single distribution switchboard. This system would be called N+1 since there is only one generator paralleling switchboard and one UPS system.

In a 2N system, there are two identical systems with only one required to carry the load. In the following example, the critical distribution system has two generating systems of two generators, each connecting to a separate generator-paralleling switchboard. It also has two systems of four UPS modules in a parallel configuration, each with a static bypass switch. Each UPS system supplies power to separate distribution switchboards. The A switchboards supply power to one side of the STS and the B switchboard supplies power to the other side. Each STS supplies power to the PDU, which consists of a step-down transformer and distribution panel. The panel supplies power to the single-cord loads. The STS is providing power to the critical load through one side of the critical distribution system (generators and UPS modules, etc.), with the other system as backup.

In the 2N system shown in Figure 15, it is common to have half of the STSs set with the preferred source as A and the other half with the preferred source as B. This prevents a 100% step load from one UPS system onto the other if the first system were to fail.

When the reliability of the individual component is the same, a system requiring one out of two components will be more reliable than a system requiring two out of three. Two complete systems will be more reliable than one system with redundant components. Therefore, a 2N system will be more reliable than an N+1 design. However, there are also economic considerations involved, which is why reliability analysis provides a useful tool in assisting with critical facility design.

In large critical facilities, the UPS system is sometimes configured as 2(N+1). An example of this is shown in Figure 16, which has two separate UPS systems of five UPS modules operating in a parallel redundant configuration. If any four UPS modules can carry the load, then each system is N+1, and since there are two systems, the overall UPS system is 2(N+1). The generating system in Figure 16, however, is N+1 since there is only one system and two out of three generators are required to carry the load.

The IT equipment shown in Figure 16 has dual cord power supplies (two power supplies, each with its own power cord in which either power supply can provide the needed energy). One cord from each power supply is powered by a separate UPS system to utilize the redundancy of the 2(N+1) configuration.

Another common UPS system configuration is distributed redundant (DR). In this configuration, there is a redundant UPS system. Shown in Figure 17 is an example of a DR system requiring two out of three UPS systems to carry the critical load.

A major advantage of the DR configuration is more of the equipment capacity can be used. With a 2N configuration, only half of the capacity can be used. With a two out of three DR configuration, two-thirds of the capacity can be used.

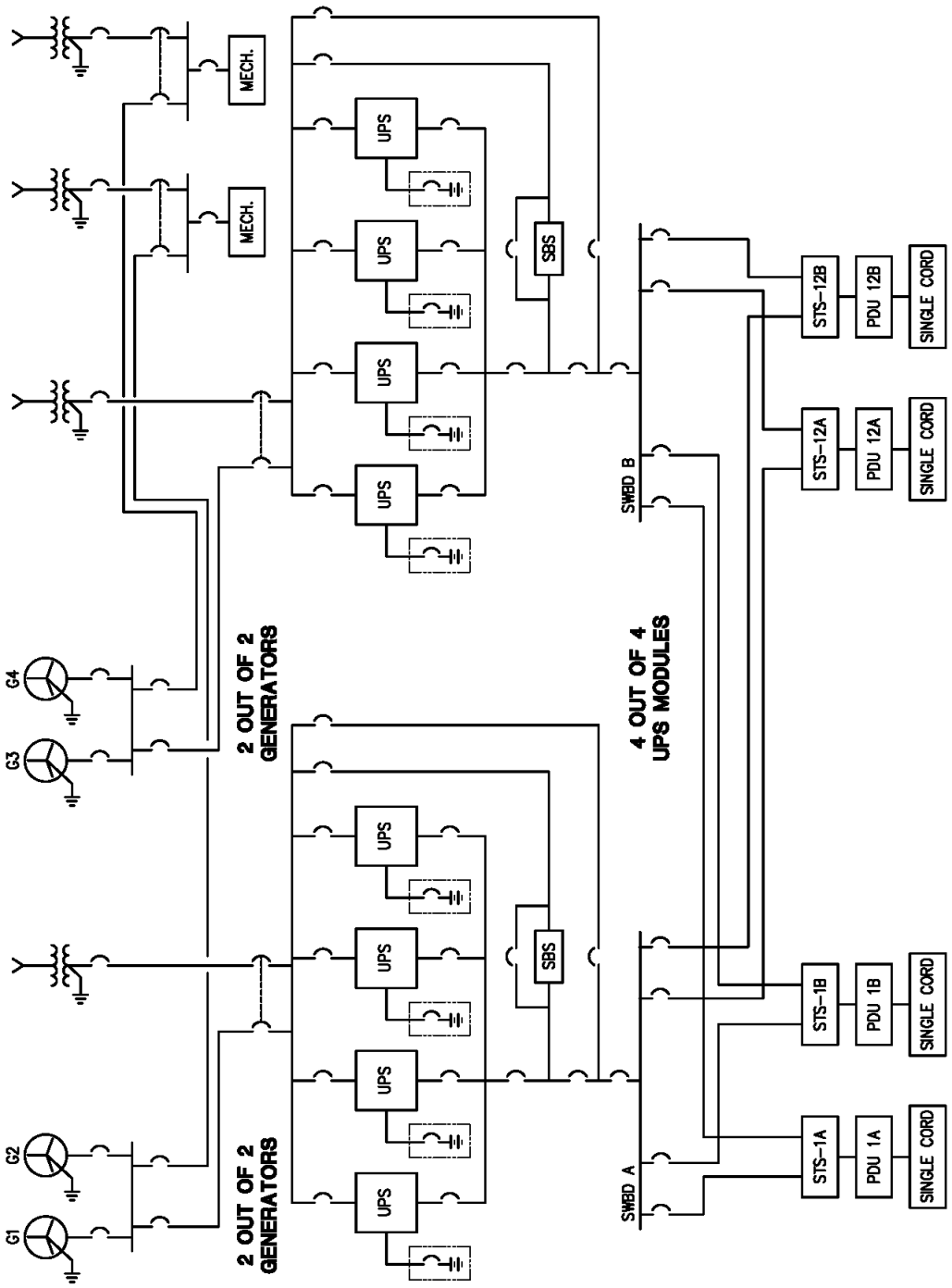

Figure 16—2N electrical distribution to single-cord loads

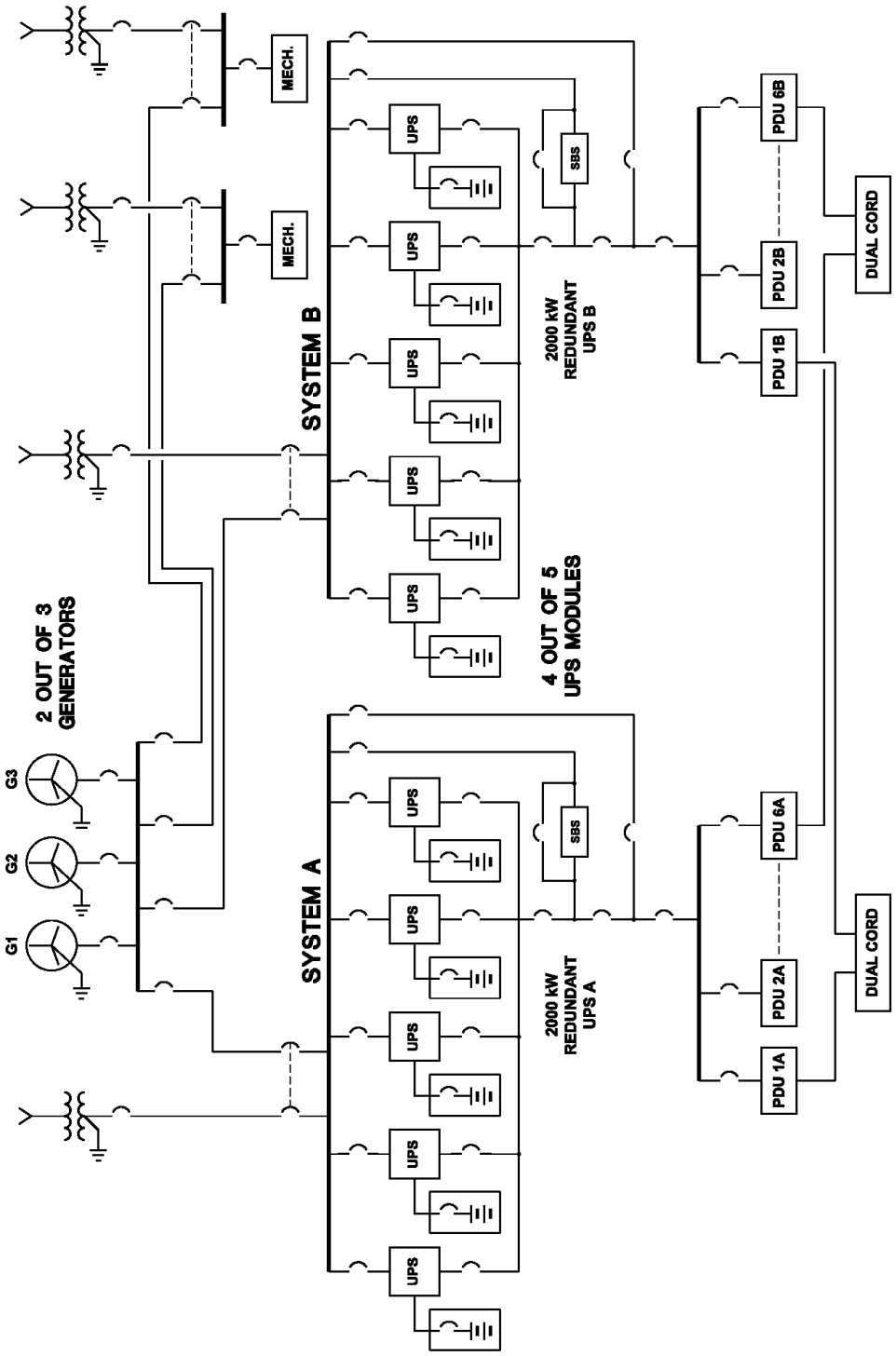

Figure 17—N + 1 generators, 2(N + 1) UPS system supplying dual cord loads

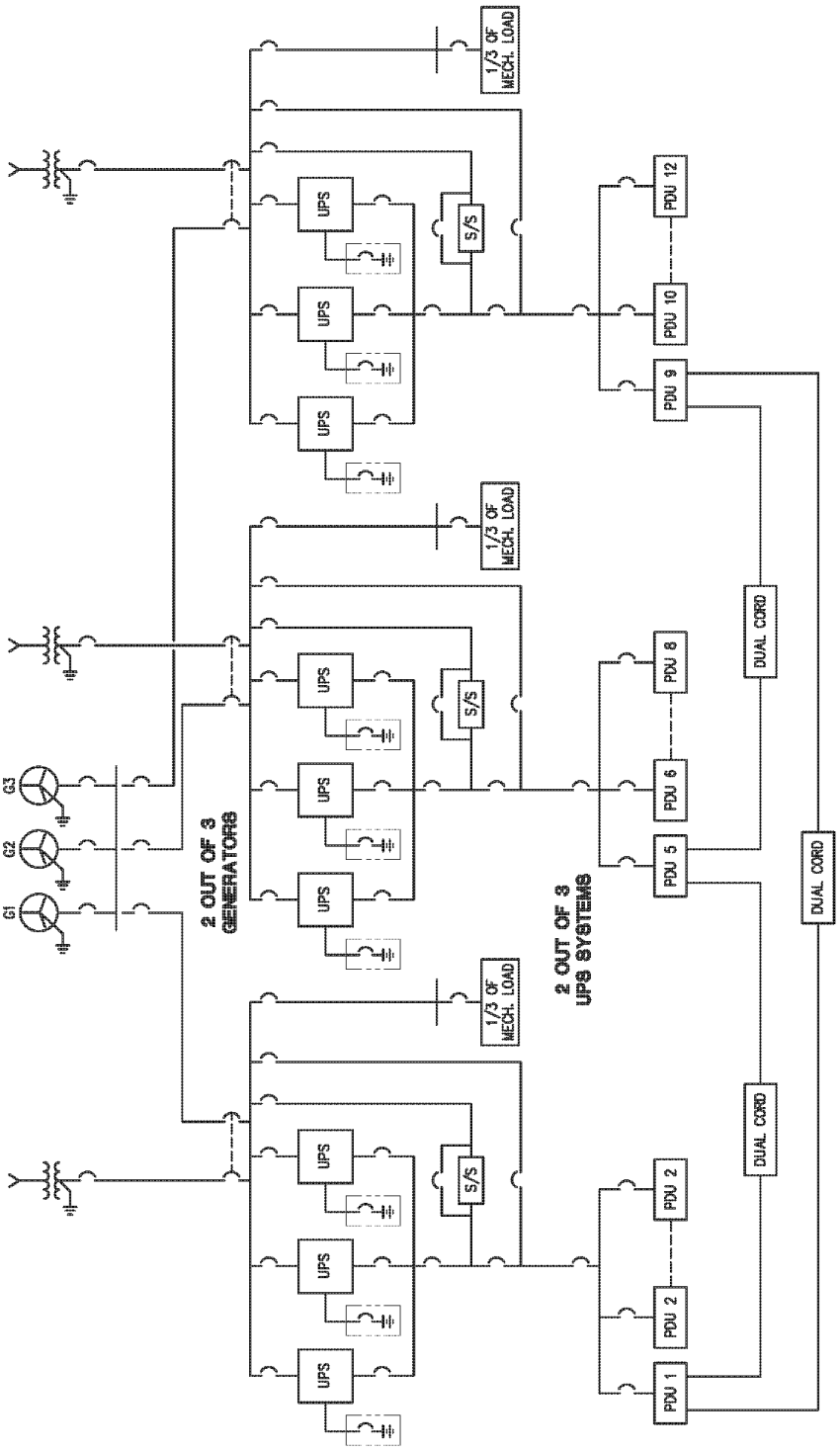

Figure 18—Distributed redundant UPS systems requiring two out of three systems

A disadvantage of the DR configuration, as compared to a 2N configuration, is that the system is slightly less reliable. Another disadvantage is the cable management for powering the IT equipment with dual cords from diverse sources is more complex. This will be discussed in more detail in 7.4.

7.3 Eliminating all single points of failure

A very successful method of improving reliability is to eliminate any and all SPOF. As discussed in 4.1.3, a SPOF is a place in the electrical distribution system in which the failure of a single piece of equipment causes the system to fail. For example, in Figure 14, the switchboard below the UPS modules that supplies power to the PDUs is an SPOF. Should there be a fault at that switchboard, all of the critical loads would lose power.

In Figure 14, the switchboard supplying power to the UPS modules could also be an SPOF. Any failure that takes longer to repair than the time period the batteries can carry the load will cause the critical loads to lose power. Therefore, a fault on the switchboard itself could take down all of the critical loads. However, the main breaker tripping on a feeder fault that could be quickly located and isolated may not take down all of the critical loads.

The purpose of going to a 2N design is to eliminate SPOF. With the 2N configuration, there is a complete second system. However, to make use of the second system, there must be a method of transferring the load from one system to the other without interrupting the operation of the load.

There are two methods commonly used to accomplish this. The first method is using STSs to transfer the power to the PDUs and racks of IT equipment from one UPS system to the other. The second method is using IT equipment that has two power supplies built into it, either of which is capable of powering the entire load (see Figure 5). This is commonly referred to as dual cord loads since there are two power cords (one for each power supply). With dual cord loads, it is important to make sure that each cord is powered from a different system, or the benefit of the redundant system is lost.

In Clause 8, it will be shown that the use of dual cord loads significantly improves the reliability over a single cord load, even when the single cord loads are fed by two systems using STSs. The use of STSs with dual cord loads improves the reliability over that of the dual cord load without STSs, but only by a small increment.

7.4 Using STSs and dual cord equipment—cable and load management

In addition to making sure the two supplies for an STS or dual cord equipment come from different sources of UPS power, it is also necessary to manage the overall load on the UPS systems. In order for redundancy to exist, there must be sufficient capacity in each of the UPS systems to carry the entire load they would receive if the other system failed. Therefore, for a 2N configuration, the maximum load each UPS system can carry in normal operation is 50% of its system rating. For the DR configuration of Figure 17, each UPS system can carry 66.6% of its system rating, *provided the load is evenly balanced between all three systems*. Figure 18 shows the proper load distribution for the DR configuration with three 1500 kW UPS systems.

Keeping track of how the dual cord loads are distributed is often referred to as cable and load management. Power cables from the PDU to the IT equipment rack are run for the dual cord loads. Specific PDUs are paired for 2N systems or grouped for systems with more than two UPS systems. The DR configuration would have groups of three PDUs, as shown in Figure 19.

Figure 17 shows the load distributed between the three PDUs. Each of the other PDUs in the figure would be similarly connected between the three systems. Then the IT equipment must also be evenly distributed between the three phases of the PDUs.

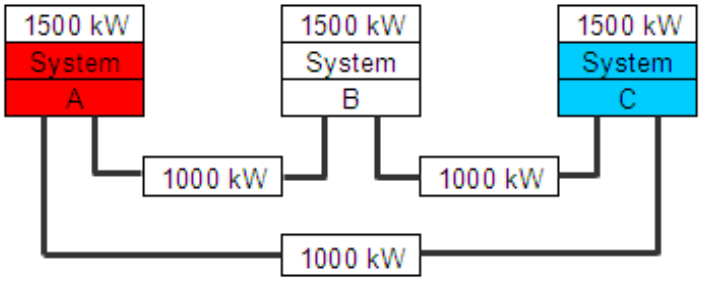

Figure 19—Load distribution for the two-out-of-three distributed redundant (DR) system

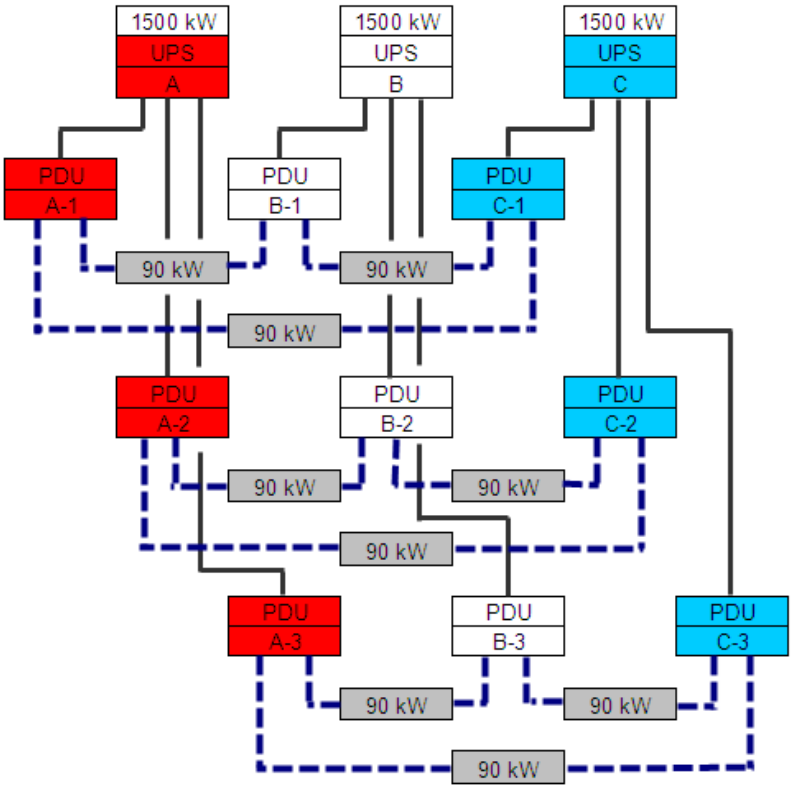

Figure 20—Dual cord load distribution for three groups of three 150 kVA PDUs in a DR configuration

8. Reliability and availability of critical distribution system configurations

8.1 Impact of redundancy on reliability calculations

In 7.4, improving reliability by eliminating SPOF and adding redundancy were discussed. Here we will provide a comparison of the critical systems discussed previously and shown in Figure 14, Figure 15, Figure 16, and Figure 17.

Table 1 shows the MTBF, MTTR, inherent availability, and the probability of failure. Reliability is the probability that a component or system will perform required functions under stated conditions for a stated period of time. It is the probability of success. The probability of failure is the complement of reliability; probability of failure = (1 – reliability). All of the probabilities of failure given in this standard are for a five year period of operation (43,800 h).

Table 1—Critical electrical distribution systems reliability for single cord loads

Name	Description of critical distribution system	MTBF (years)	MTTR (hours)	Inherent availability	Probability of failure
Figure 14: N+1 (GEN + UPS)	Gen (2-3), UPS (4-5) 12 single cord loads	7.4	11.29	0.9998253	49.11%
Figure 15: 2N (GEN + UPS)	2X [Gen (2-2), UPS (4-4)] 12 STS/PDU single cord loads	8.9	10.96	0.9998592	39.82%
N+1 GEN 2(N+1) UPS	Gen (2-3), 2X [UPS (4-5)] 12 STS/PDU single cord loads	8.9	11.06	0.9998576	39.47%
N+1 Gen: DR (2-3) UPS	Gen (2-3), DR (2-3) X [UPS (2-3)], 12 STS/PDU single cord loads	8.7	11.08	0.9998549	40.71%

Probability of failure is used in place of reliability to emphasize that it is a measure of the likelihood of a failure occurring during a specific time interval. MTBF, MTTR, and A_i are not functions of time, but reliability and probability of failure are time dependent. The values shown are for five years of operation.

An RBD was made for each the systems in a software program. The failure rates used for the components are from IEEE Std 493™ (*IEEE Gold Book™*). The values shown in Table 1 are representative of the system design, not absolute calculations. The accuracy shown (e.g., to seven figures) is just a function of the software program's capability to perform statistical calculations, not the accuracy of the results.

It should also be noted that the probability of failure values given in Table 1 are for any one single-cord of the group of 12 failing. As discussed in 8.2, the system is modeled in this manner to be an indication of the probability of losing all the loads on a PDU, not all the loads in the data center.

For the N+1 system shown in Figure 14, A_i is 0.9998253. Essentially that would mean that the system is likely to experience one outage in 7.4 years that lasts for 11.2 h. As discussed in 6.1, this would be far better than an outage every year that lasts for 1.5 h. Yet both would have the same A_i.

That the reliability is significantly improved by eliminating SPOF can easily be seen by comparing the previous three configurations, 2N, 2(N+1), and the 2 out of 3 DR with STSs and single cord loads in Table 1 to the same three system with dual cord loads in Table 2. In each of the three cases, the difference between the systems with STS/single cord loads to the systems with dual cord loads is just one SPOF—the STS. Yet in each case, the probability of failure is reduced by a factor approaching 2 (an average of about 1.7).

Table 2—Critical electrical distribution systems reliability for dual cord loads

Name	Description of critical distribution system	MTBF (years)	MTTR (hours)	Inherent availability	Probability of failure
2N Gen 2N UPS	2X [Gen (2-2), UPS (4-4)] 12 dual cord loads	68.9	2.57	0.9999958	6.96%
N+1 Gen 2N UPS	N + 1 Gen (2-3), 2N UPS(4-4) 12 dual cord loads	66.6	2.50	0.9999957	7.57%
Figure 16: N+1 Gen 2(N+1) UPS	Gen (2-3), 2X [UPS (4-5)] 12 dual cord loads	67.5	2.50	0.9999958	7.18%
Figure 17: N+1 Gen DR (2-3) UPS	Gen (2-3), DR (2-3) X [UPS 2-3], 12 dual cord loads	65.9	2.52	0.9999956	7.69%

The 2N system is the most reliable. However, the differences between all of the systems are very slight. The generators are only in service when the utility fails. For the previous examples, the MTBF of the utility is 4478 h, and the MTTR is 1.32 h. Therefore, the generators on the average are needed twice a year for about an hour and twenty minutes each time. Since there is generator redundancy in both systems, it is highly likely that the generators will be available when needed.

There are multiple UPS systems in each design also. Therefore, the odds of two systems failing at the same time are very slight. There is a little greater chance of losing two of the three systems than losing two of two, so the 2N and 2(N+1) are both slightly more reliable than the DR system.

There are several other common designs used in data centers in addition to the ones shown previously. Figure 20 shows a design called block redundant (BR). Each system (block) consists of utility and generator power for a pair of UPS modules. There are three primary systems and one reserve system in this example, so 75% of the capacity of the equipment is available to carry load and 25% is in a standby mode as reserve.

Figure 21 shows another design called redundant reserve (RR), which uses the same configuration for UPS power. The RR system has the same N+1 generator system used with the 2N and DR UPS configurations.

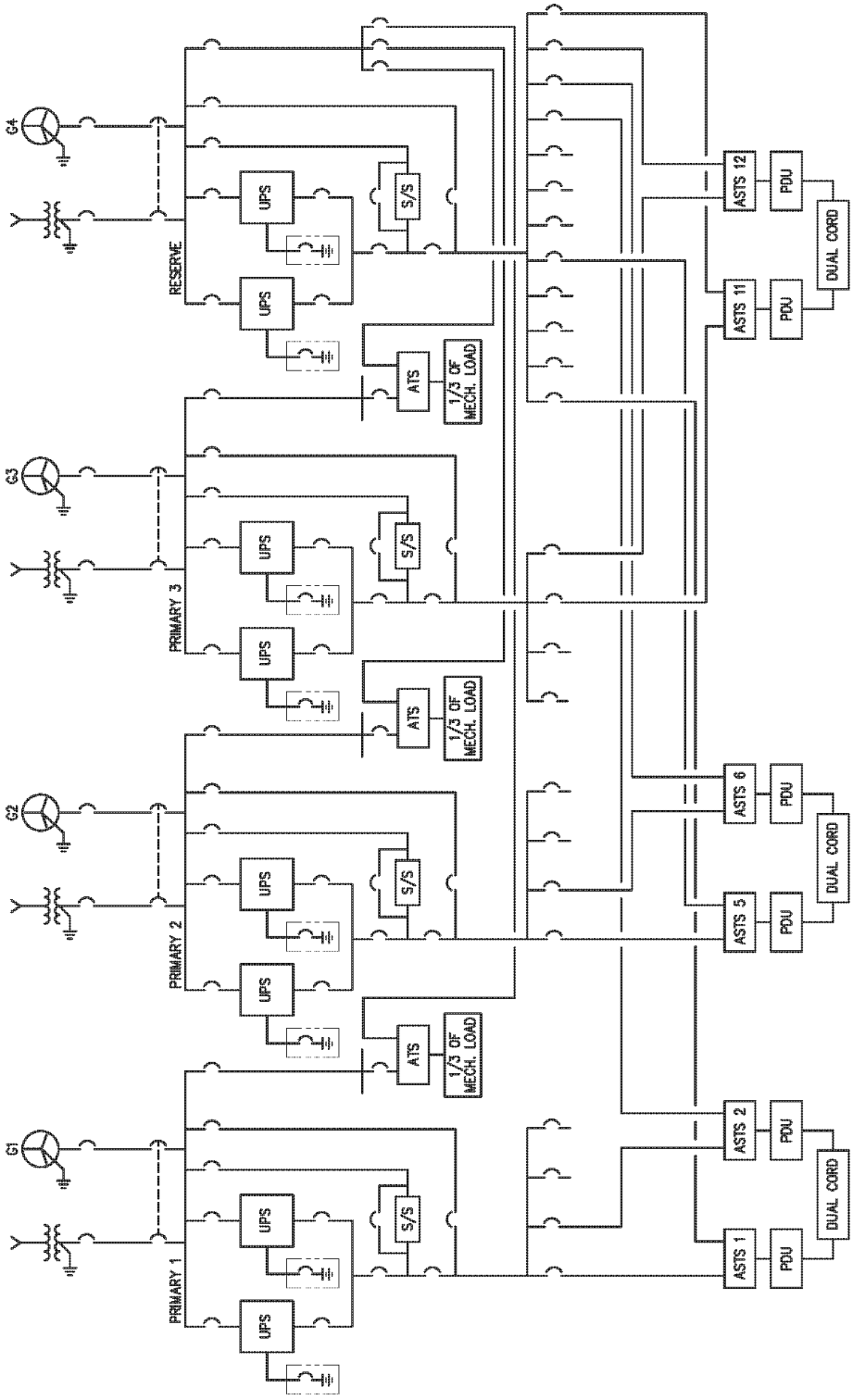

Figure 21—Block redundant (BR) configuration using STSs and dual cord loads

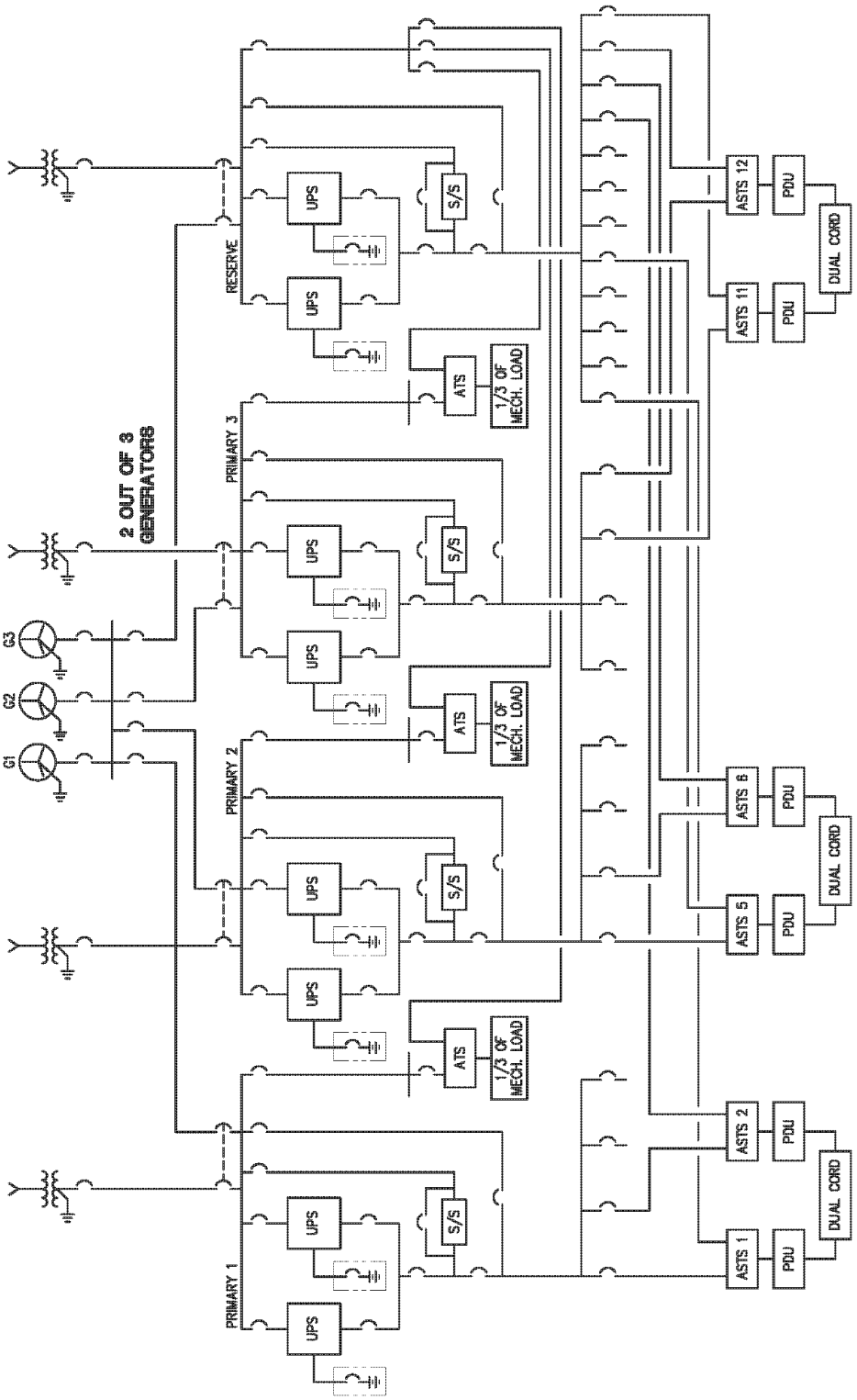

Figure 22—Redundant reserve (RR) configuration using STSs and dual cord loads

Table 3 shows the reliability calculations for the BR system, RR system, along with the DR, 2N and 2(N+1) UPS systems using STSs and dual cord loads. The BR and RR configurations require STSs to utilize the design redundancy. The DR, 2N, and 2(N+1) UPS configurations can use dual cord loads with or without STSs. By comparing the reliability values from Table 2 and Table 3, it can be seen that the STS increases the reliability a small amount over dual cord loads alone.

Table 3—Critical electrical distribution systems with STSs and dual cord loads

Name	Description of critical distribution system	MTBF (years)	MTTR (hours)	Inherent availability	Probability of failure
Figure 20 N+1 Gen BR (3-4)	Gen (3-4),BR (3-4) X [UPS (2)], 12 STS/PDU dual cord loads	50.0	4.80	0.9999891	7.81%
Figure 21 N+1 Gen RR (3-4) UPS	Gen (2-3),RR (3-4) X [UPS (2)], 12 STS/PDU dual cord loads	67.8	2.00	0.9999966	6.88%
N+1 Gen DR (2-3) UPS	Gen (2-3), DR (2-3) X [UPS (2-3)], 12 STS/PDU dual cord loads	80.0	2.20	0.9999969	6.09%
N+1 Gen 2N UPS	Gen (2-2), 2X 2N UPS (4-4) 12 STS/PDU dual cord loads	81.2	2.22	0.9999969	6.02%
N+1 Gen 2(N + 1) UPS	Gen (2-3), 2X 2(N+1) UPS (4-5) 12 STS/PDU dual cord loads	81.4	2.19	0.9999969	5.66%

8.2 Impact of facility size on reliability calculations

As mentioned in the earlier subclauses, the larger the facility, the lower the reliability will be just because there are more parts to fail. Table 4 shows an example of this using N+1 generators (3) 2N UPS system (4) with 12 dual cord loads. The first row is the reliability of system given previously in Table 2. The second row shows the same system with 24 dual cord loads instead of 12 in the RBD. The third row shows two complete systems of (N+1 generators (3) 2N UPS system (4) with 12 dual cord loads).

In comparing the first set to the second, the reliability is dropped dramatically by doubling the number of critical loads connected to the UPS modules. The third set shows that essentially doubling the size of the 2N facility also drops the reliability significantly.

This example shows that it is very important to keep the models consistent when comparing one configuration to the next. In the comparisons done for Table 1, Table 2, and Table 3, a critical load of 3000 kW was used. Therefore the UPS modules would have to be 750 kW for the N+1, 2N, and 2(N+1) designs, but only 500 kW for the DR, BR, and RR designs.

The above example also shows that for a large data center with multiple identical systems, the proper method is to model one system and use the reliability and availability values obtained from the one system as typical for the facility. Otherwise a large, very well designed data center will have the reliability and availability values more properly associated with a poorly designed, small data center just because it is large.

Table 4—Impact of facility size and number of loads on reliability and availability

Name	Description of critical distribution system	MTBF (years)	MTTR (hours)	Inherent availability	Probability of failure
N+1 Gen 2N UPS 12 DCL	N + 1 Gen (2-3), 2N UPS(4-4) 12 dual cord loads	66.6	2.50	0.9999957	7.57%
N+1 Gen 2N UPS 24 DCL	N + 1 Gen (2-3), 2N UPS(4-4) 24 dual cord loads	35.7	2.62	0.9999916	12.89%
2X (N+1 Gen 2N UPS)	2X(N + 1 Gen (2-3), 2N UPS(4-4) 12 dual cord loads)	34.2	2.56	0.9999915	12.96%

8.3 Operational availability vs. inherent availability

As discussed in IEEE Std 493™ (*IEEE Gold Book™*), there are two common measures of availability: inherent availability (A_i) and operational availability (A_o). The difference between the two is based on what is included as repair time. For A_i, only the time it takes to fix the equipment is included. A_i assumes that the technician is immediately available to work on the equipment the moment it fails and that he has all the parts, etc. necessary to complete the repair. For A_o, all the delays for scheduling, travel time, parts, etc., are included. If it takes 24 h to fly a part in to repair the equipment, that adds to the repair time.

A_i and A_o show different aspects of the system being analyzed. A_o would be the real world—how the system really operates. There are usually delays between the time a piece of equipment fails and when the repair begins. Spare parts inventories are also very significant and directly impact A_o. Therefore, when determining spare parts inventories, on-site personnel and their level of training, etc., A_o is a useful tool.

In some commercial 7×24 facilities, it is common for maintenance to be done by outside contractors working under service level agreements. It is possible to use reliability modeling to produce a cost/benefit analysis of service level agreements and spare parts stocked. A certain quantity of critical spares held on-site at a particular cost would improve the total time for repair, which in turn would improve the A_o.

A_i is a more useful tool in analyzing the system design. Since there are wide variations in the maintenance practices from facility to facility, A_o could vary significantly between two facilities with identical infrastructures. Eliminating all of the logistics involved with getting the parts and trained individuals to the piece of equipment, and counting only the actual repair time, provides a more accurate comparison. It shows the availability that is inherent to the design if the spare parts inventory and repair are perfect.

9. Critical mechanical cooling systems

It is common knowledge that momentary interruption of the electrical power is a significant failure the critical load must be protected from. UPS and standby generators are very common for a facility with IT loads considered critical. Special cooling equipment is also required where there is a significant amount of IT equipment.

Unlike the electrical power, loss of cooling is not an immediate failure. It takes some time for the IT equipment to overheat. This is discussed in more detail in 5.4 and 5.5.

9.1 Cooling equipment commonly used

9.1.1 Water-cooled chiller

There are two primary sections to a water-cooled chiller: the refrigeration section and two tube-bundle heat exchangers. The refrigeration section uses a compressor, expansion valve, and special refrigerant (such as R10A, R22, R401, HCFC 123, etc.). The compressed refrigerant flows through the expansion valve, becoming a gas, and cooling the exterior of one tube bundle (evaporator). The chilled water flows through the tubes of this bundle to the cooling units in the data center.

The warm refrigerant (from the evaporator) is then forced in to the second tube bundle (condenser) by the compressor. The compression of the refrigerant causes its temperature to increase. The elevated temperature is reduced by the condenser tube bundle, allowing the refrigerant to change states back into a liquid. The water flowing through the second tube bundle absorbs the heat. This water (called condenser water) is pumped over the cooling tower by the condenser water pump (CWP).

Figure 23—Water-cooled chiller

9.1.2 Air-cooled chiller

The chilled water side of an air-cooled chiller works the same as a water-cooled chiller. However, for the air-cooled chiller, the condenser coils dissipate the heat directly. The air-cooled chiller is mounted outside, and fans blow air across the condenser coils to dissipate the heat. In Figure 23, cooling coils are shown along the side, and there are internal fans that blow air out of the top. The heat exchanger, compressor, expansion valve, etc. are below the condenser coils.

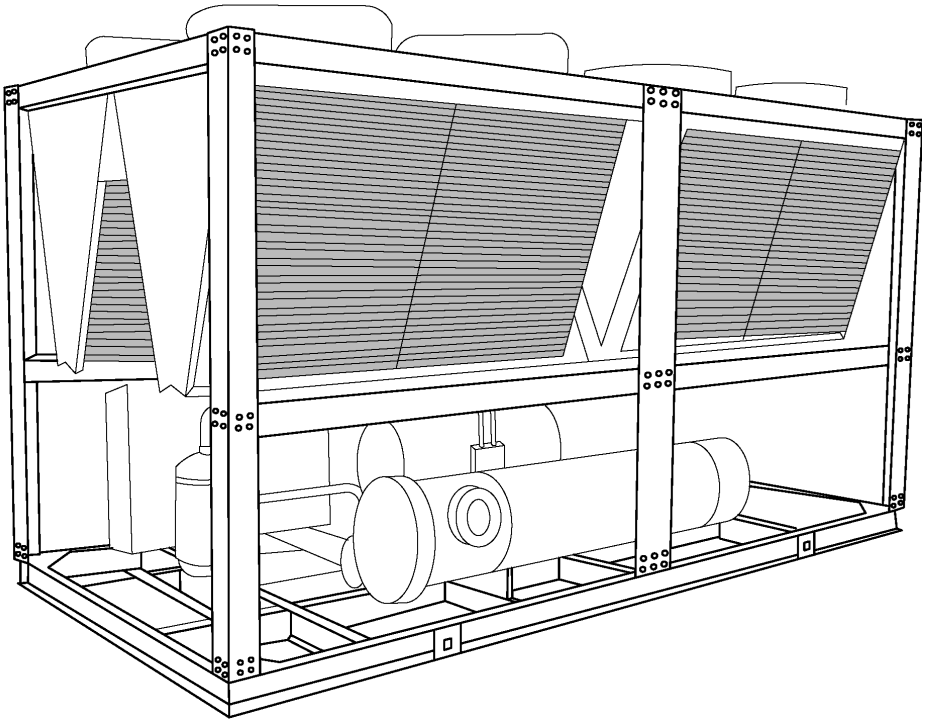

Figure 24—Air-cooled chiller

9.1.3 CRAC unit with air-cooled condenser

An air-cooled condenser is used with one type of CRAC direct expansion (DX) unit (see 4.3.1). It is very similar to the condenser for an air-cooled chiller. The refrigerant from cooling the cooling (evaporator) coils in the CRAC DX unit is compressed back into a liquid and piped outside to dissipate the heat through the condenser coils with fans blowing air across them.

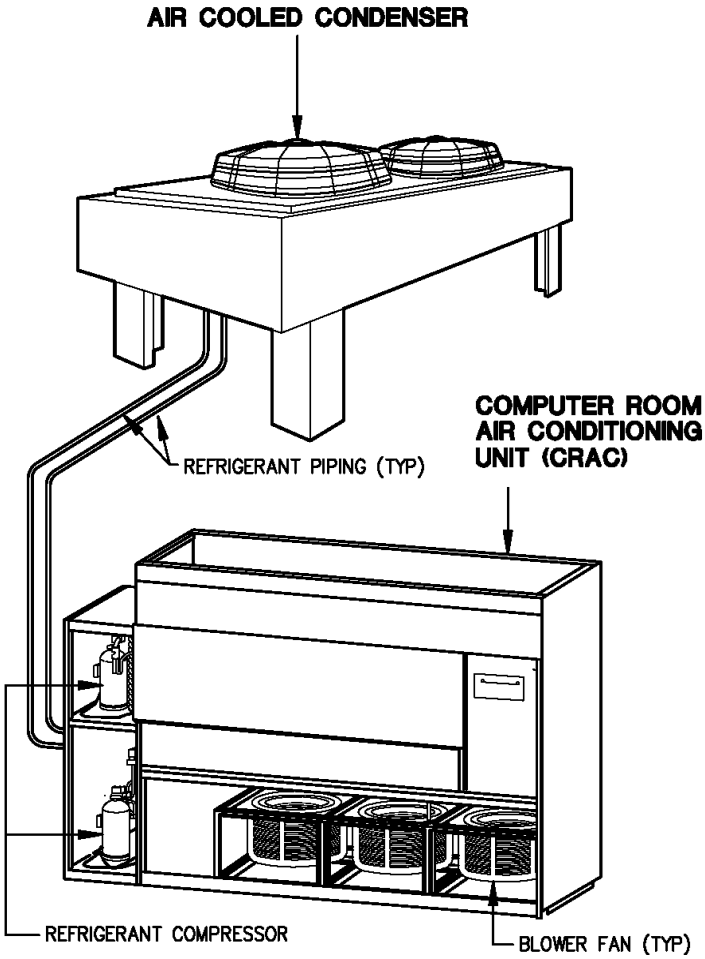

Figure 25—CRAC unit with air-cooled condenser

9.1.4 Drycooler

For a CRAC DX using a drycooler, a shell and tube condenser is used, which is mounted inside the CRAC DX unit. A water/glycol mix is pumped through the shell side of the condenser, picking up heat which it dissipates flowing through cooling coils in the drycooler. Like the air-cooled condenser, the drycooler has a fan that blows air across the cooling coils to reject the heat. This type of CRAC DX unit can also be used with a cooling coil in an evaporative cooling tower to reject the heat.

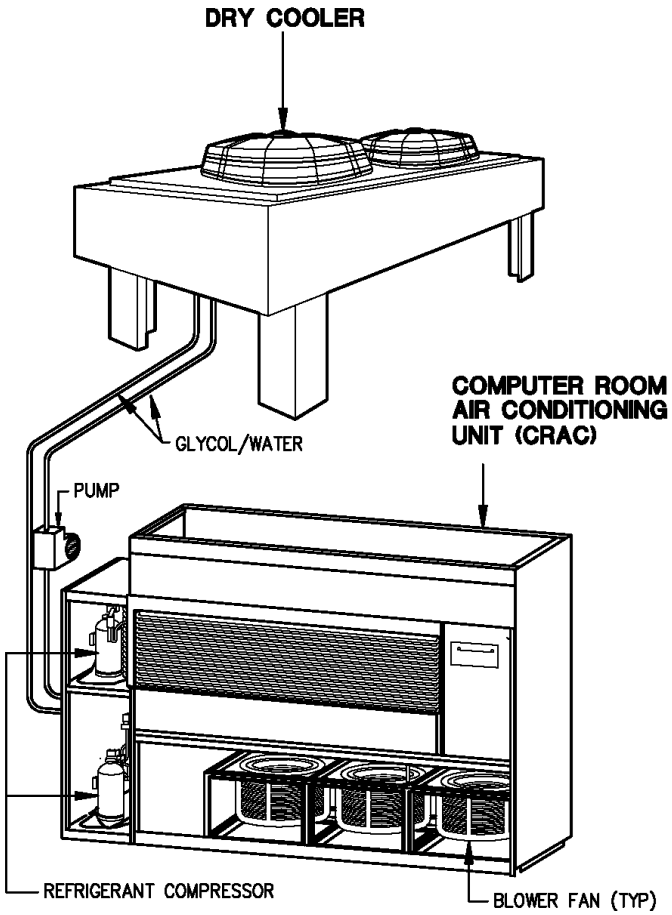

Figure 26—CRAC unit with drycooler

9.2 Common configurations of the mechanical cooling system

9.2.1 Water-cooled chiller plant

Figure 26 shows a typical mechanical cooling system used for data center cooling. It consists of a chilled water central plant of the same type of equipment used for heat, ventilation, and air conditioning (HVAC) applications. The heart of the system is the chiller, which removes the heat from the water in the chilled water loop and places it in the condenser water going to the cooling tower. The CWP pumps the water over the cooling tower.

The cooling tower works by evaporative cooling. The water is pumped over the top of the tower, which has louvers for the water to cascade over. There is also a fan pulling air from the outside of the cooling tower and exhausting upward over the tower, which helps to extract the heat from the water. Cooling towers use a significant amount of water to make up for losses from evaporation and to maintain the proper water chemistry. (The cooling tower requires periodic flushing to eject the excess chemicals that would otherwise build up in the water.)

There is always at least one set of pumps in the chilled water loop. In many designs there are two sets. The first set is the primary chilled water pumps (PWP), which pump the water through the chilled water tube bundle of the chiller and out into the chilled water loop. If the design does not include a second set of pumps, the PWP also pumps the water through the computer room air handling (CRAH) units.

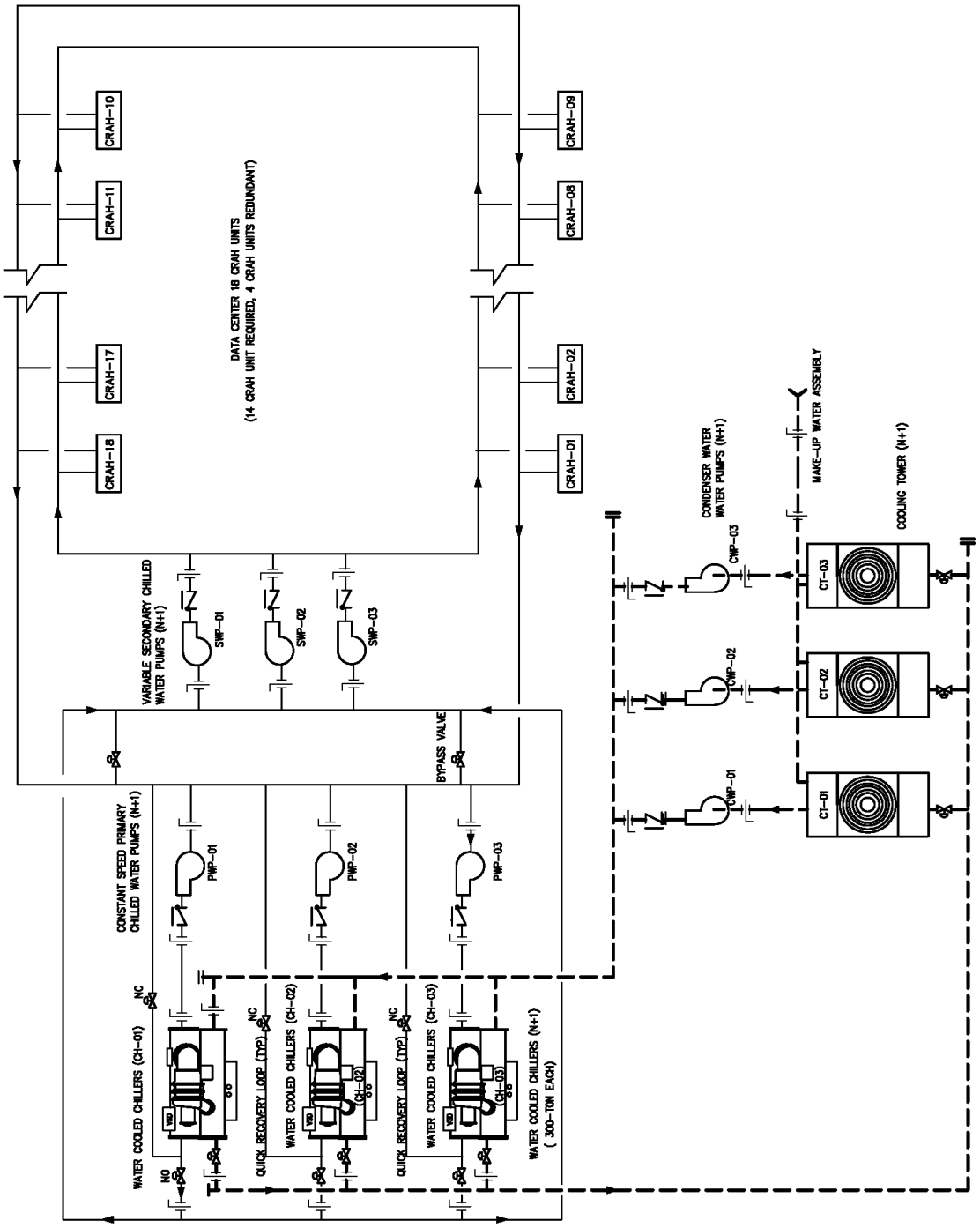

Figure 27—Typical chilled water central plant used for data center cooling

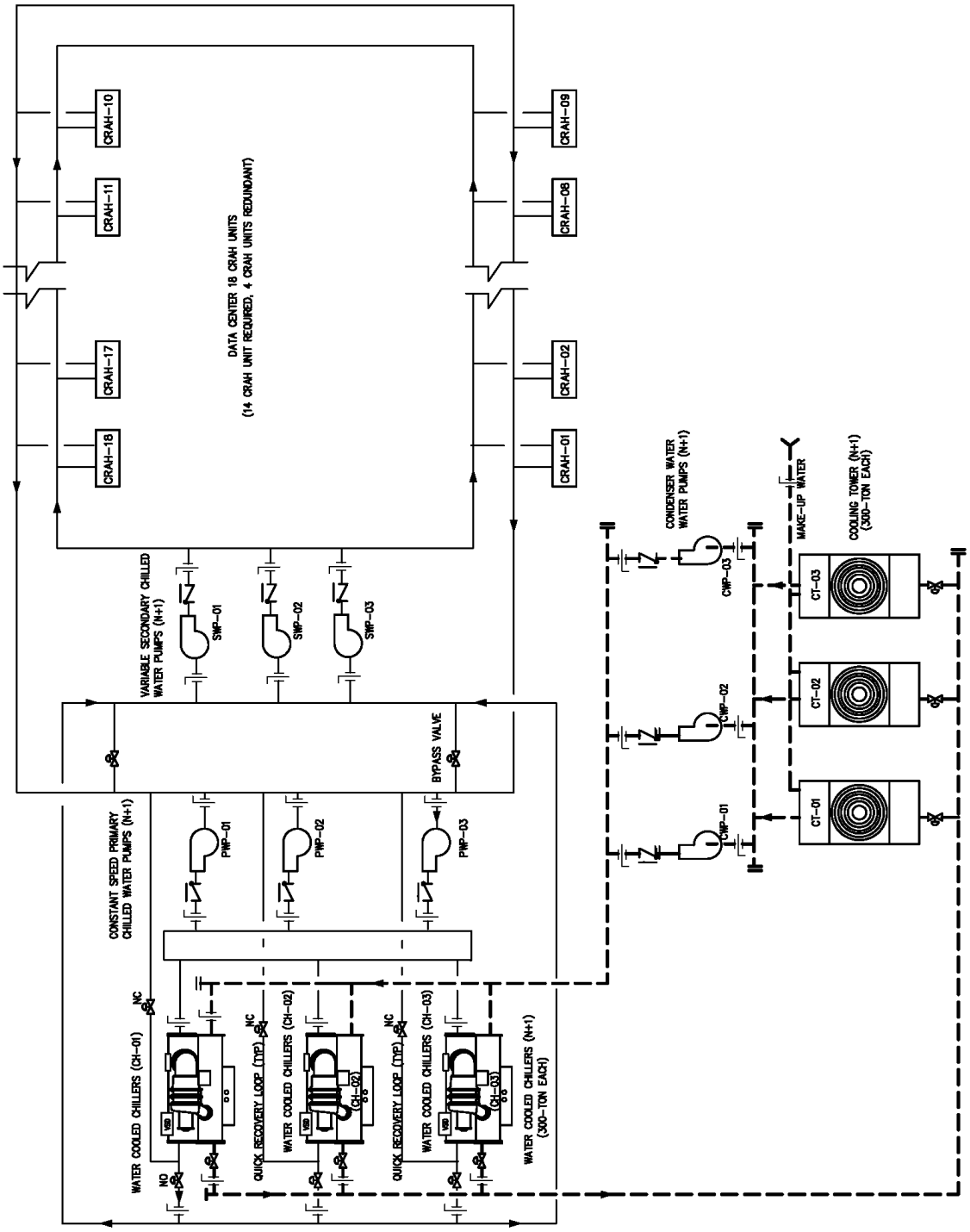

Figure 28—Chilled water central plant with common header to pumps

For designs that do use secondary chilled water pumps (SWP), there is a bypass loop which decouples the primary and secondary chilled water loops. (If the system is designed properly, the primary chilled water loop has slightly more water flowing in it than the secondary chilled water loop, and the excess amount of water flows through the bypass loop.)

To improve the reliability of the system and to make it concurrently maintainable, loops and isolation valves are added to the main piping. For data centers with high density to the IT equipment load (200 W/ft^2 or greater) the recovery time for the chillers to restart after a power outage is often too long. A common solution is to add a thermal storage tank. The thermal storage tank provides additional chilled water (in addition to what is already in the chilled water piping) to slow the temperature rise in the chilled water loop and, ultimately, the data center. The thermal storage tank can also provide a back-up water supply for the cooling tower should city water be lost for a significant amount of time.

9.2.2 Air-cooled chiller plant

Figure 28 shows a typical air-cooled chilled water plant. The main advantage of an air-cooled chiller is that very little make-up water is required for operation. A cooling tower requires a significant amount of water to operate, so loss of city water over an extended period of time can force a water-cooled chiller to be shut down. An air-cooled chiller does not need make-up water, as the chilled water is a closed loop system. The main disadvantage of an air-cooled chiller is it requires more energy to operate; thus it can be more expensive (depending on the cost of electricity and water for the facility).

To take advantage of the efficiency of a water-cooled chiller and at the same time avoid failure of the cooling system due to loss of make-up water, some designs use both types of chillers. When make-up water is available, the water-cooled chiller is used. If city water is lost, the air-cooled chiller is used. Such a system is shown in Figure 29. For this system, the water-cooled chiller is twice as large as the air-cooled chillers, so either the water-cooled chiller or both air-cooled chillers are required to provide the data cooling load on a design day.

9.2.3 CRAH unit distribution

Figure 30 shows a typical layout for the CRAH units along both walls of the data center. The data center room has a raised floor, and the plenum below the data center floor is used to distribute the cold air from the CRAH units. The rows of IT equipment are set up in a hot aisle/cold aisle configuration in which the front side of each row of IT equipment faces the front side of another row of IT equipment. Perforated tiles (floor tiles with holes in them) are put in the aisle between the two rows of equipment with the front sides facing each other. This is a cold aisle since the perforated tile let the cool air from the CRAH units into the room in this aisle. The back sides of the IT equipment are also set up facing the back side of another row of IT equipment. The cooling fans inside the IT equipment pull the cold air from the front through the equipment and out the back. Since the cool air picks up the heat from the IT equipment as it flows through it, the rows with the back sides of the IT equipment facing each other are the hot aisle. In Figure 30, the CRAH units are lined up with the cold aisles.

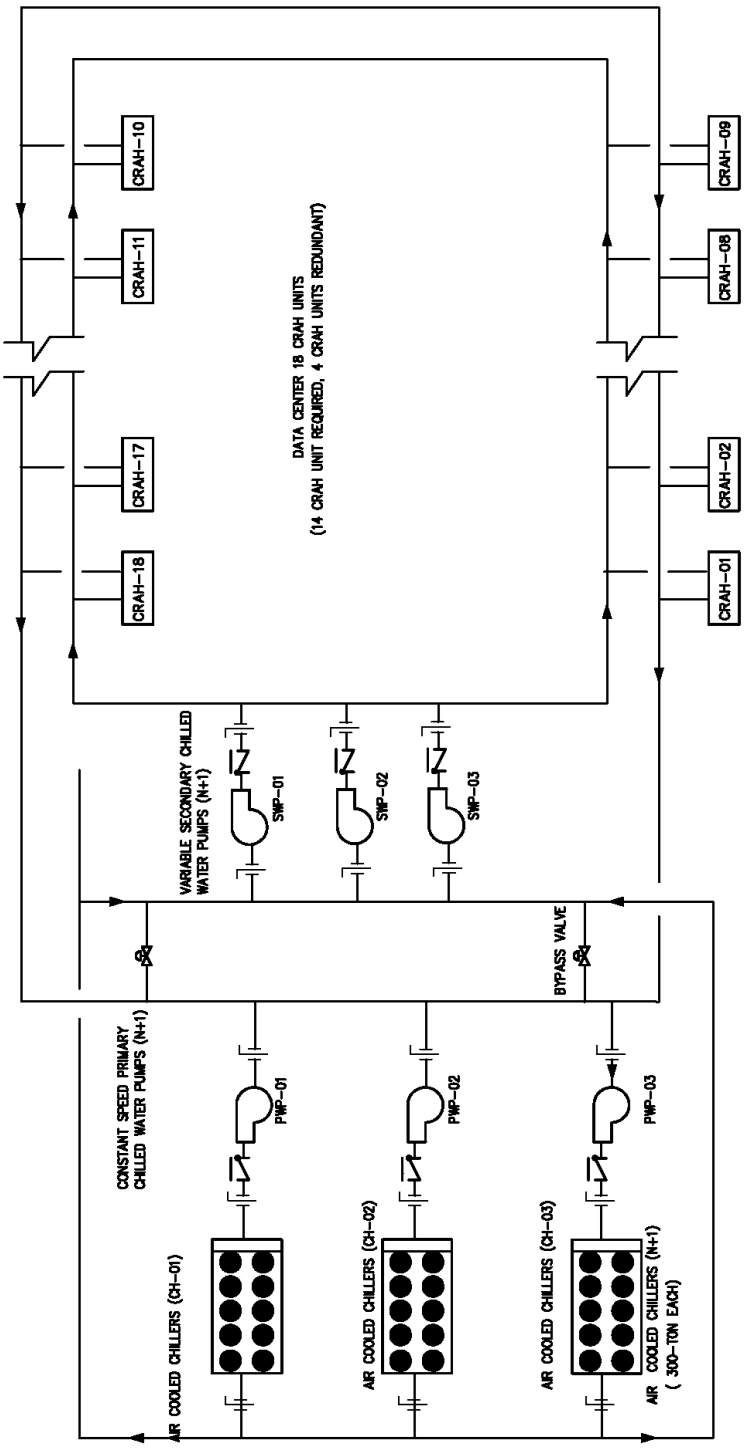

Figure 29—Air-cooled chilled water plant

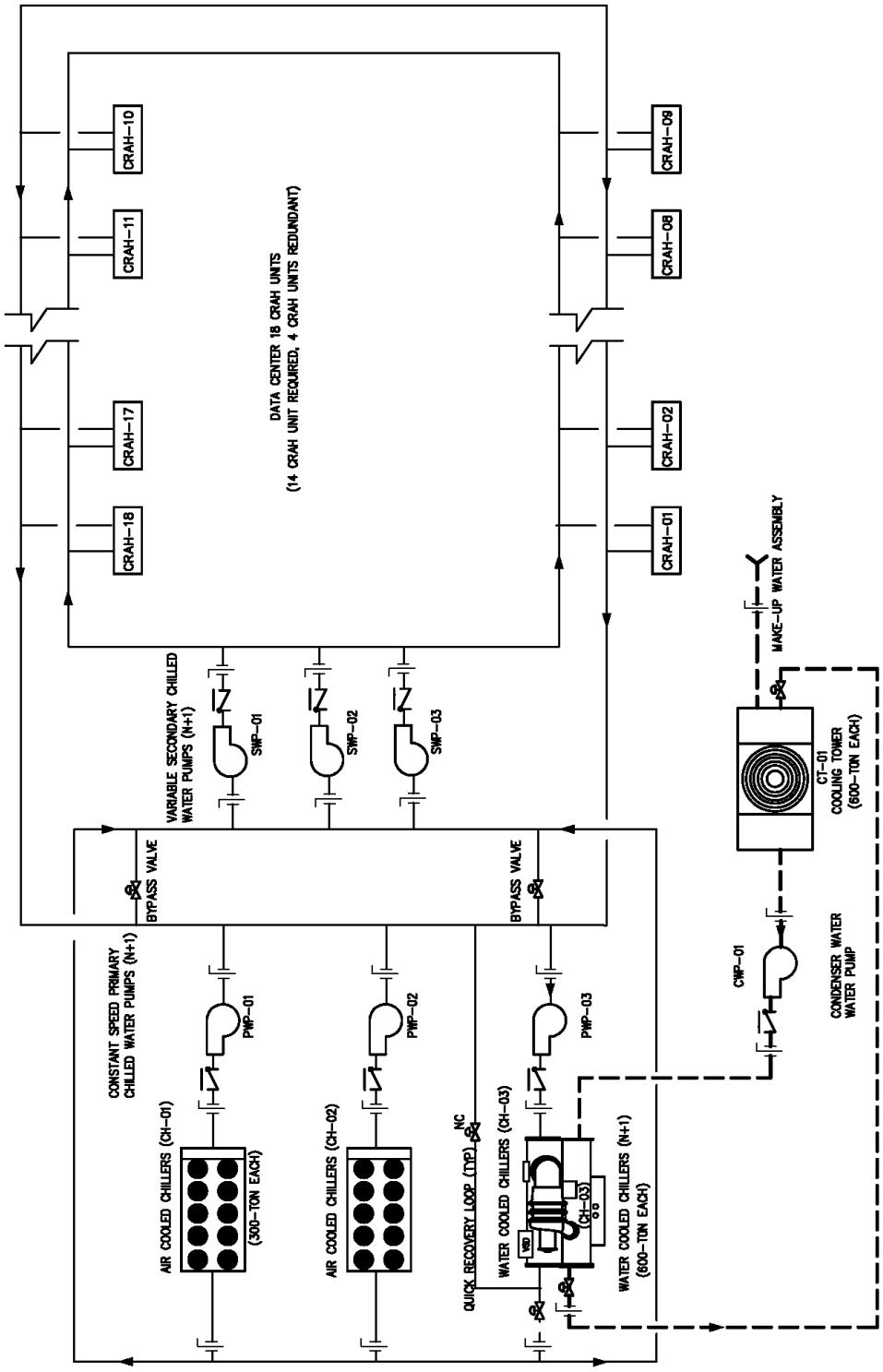

Figure 30—Air-cooled and water-cooled chilled water plant

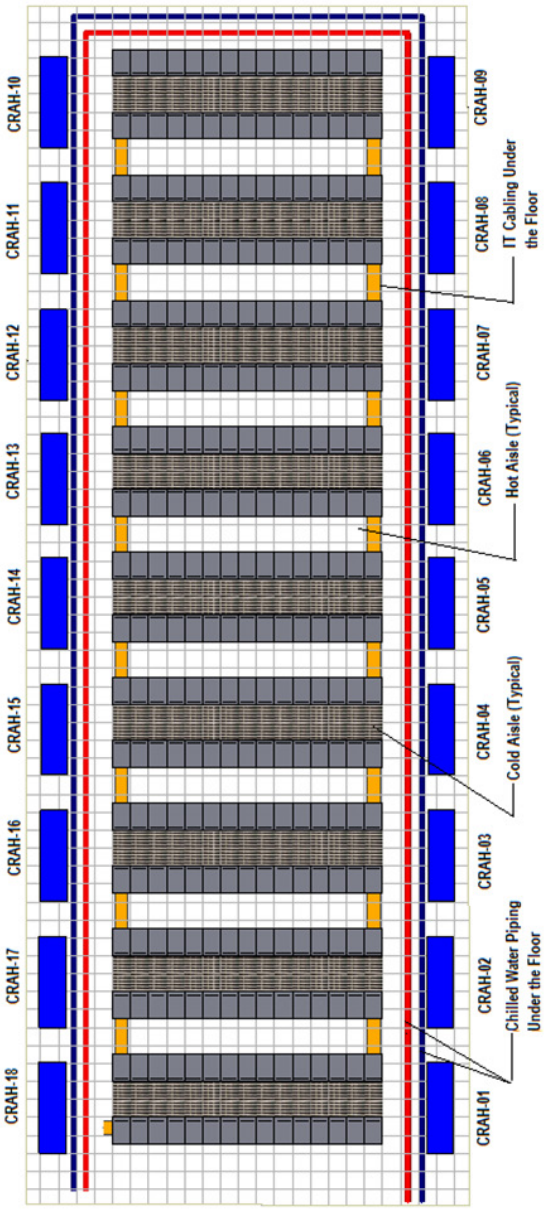

Figure 31—CRAH units distributed along both sides of the raised floor

9.3 Reliability of the critical mechanical cooling system designs

The reliability of the mechanical cooling systems based on the type of mechanical equipment used is shown below in Table 5. Since three of the four designs require make-up water to operate, loss of water has been included in the RBD. However, actual failure and repair data for city water is not readily available in most areas. Therefore a MTBF of 20 years and an MTTR of 6 h were arbitrarily selected as a reasonable estimate.

Another important point to keep in mind is that this analysis includes only the controls as a part of the major assemblies. For example, the block that represents the chiller in the RBD contains the part HVAC controls as part of the assembly. The overall building management system (BMS) controls that are normally used to control a large chilled water cooling system (see 9.6) have not been included.

In the comparison below for Figure 26 and Figure 27, the analysis shows that the system is slightly more reliable if any CWP can be used with any cooling tower and any chiller, and if any PWP can be used with any chiller. This makes sense from a mechanical equipment inspection. The CWP for chiller #1 could fail at the same time as PWP #2 failed. For the system in Figure 26, that would constitute a failure for the cooling system as a whole. However, since the system in Figure 27 can use any pump with any chiller, it would not fail as a cooling system.

What is not included in that analysis is that the BMS controls that are required to use any pump with any chiller are far more complex than the controls that are required when the pumps are dedicated to a specific chiller. It is very important to keep the reliability analysis in its proper perspective for it to be a useful tool in determining the overall best design for a specific application.

Table 5—Reliability and availability of mechanical cooling systems

Name	Description of critical distribution system	MTBF (years)	MTTR (hours)	Inherent availability	Probability of failure
Figure 26	2 of 3 [CT, Dedicated (CWP, WC CH, PWP), SWP] + (14 of 18) CRAH units	77.9	6.65	0.9999903	1.72%
Figure 27	2 of 3 [CT, CWP, WC CH, PWP, SWP] + (14 of 18) CRAH units	78.1	6.60	0.9999904	1.62%
Figure 28	2 of 3 [AC CH, PWP, SWP] + (14 of 18) CRAH units	495	13.46	0.9999969	0.95%
Figure 29	1 [CT, CWP, WC CH, PWP] + 2 [AC CH, 2 PWP] + (2 of 3 SWP) + (14 of 18) CRAH units	226	8.96	0.9999955	2.17%

9.4 Electrical power to the critical mechanical cooling system

As discussed in earlier subclauses, many data center designs may accommodate momentary interruptions in cooling but cannot sustain an extended loss of cooling. The electrical distribution to the mechanical cooling equipment can present an overlooked single point of failure (SPOF) to the critical cooling system if not carefully considered and designed accordingly. Redundant components, piping, and isolation valves are intended to allow the system to operate with at least N capacity during a design level of component failures or isolation for maintenance. However, if all power is provided by a single motor control center (MCC), or all MCCs receive power from a single distribution point, that common single distribution point represents a SPOF to the critical cooling system that can take down the entire cooling system and ultimately the data center.

A typical problem is that the redundancy of the power to the cooling equipment does not match the redundancy of the mechanical cooling system. For example, take a 2N critical electrical distribution system similar to what is shown in Figure 15. If a two out of three mechanical cooling system is used with it, such as shown in Figure 26, a potential problem exists. Two sets of cooling towers, chillers, and pumps are powered by the A side, and the remaining set of cooling towers, chillers, and pumps are powered by the B side. If the B side fails, there is no problem since there are two sets of equipment powered by the A side. What if the A side fails? Now there is insufficient cooling equipment to prevent the IT equipment from overheating.

The most obvious solution is to install automatic transfer switches (ATSs) to one set of cooling towers, chillers, and pumps as shown in Figure 31. That way two of the three cooling systems would still be available if power was lost to one distribution system.

A better solution would be install a circuit breaker transfer pair with an ATS controller for each of the switchboards that supplies power to the mechanical cooling system as shown in Figure 32. That way power would always be available to at least two sets of cooling towers, chillers, and pumps regardless of whether or not a chiller was down for maintenance when the power failed.

A more subtle issue with the powering of cooling equipment for the IT equipment concerns power to the CRAC/CRAH units. The typical basis of design for CRAC/CRAH units is N+20% or N+25%. At N+20%, for every five CRAC/CRAH units, there is a sixth unit which is redundant. At N+25%, for every four CRAC/CRAH units, there is a fifth unit which is redundant. In either case, there are two factors regarding the power to the CRAC/CRAH units which must be taken into account. The first factor is that the panels, switchboards, etc. that supply power to the CRAC/CRAH units should be arranged in such a manner that a failure of any one panel, switchboard, etc. does not cause more than the number of CRAC/CRAH units which are redundant to be without power. The second factor is the power to the CRAC/CRAH units should be distributed so that a failure of any one panel, switchboard, etc. does not cause a loss of power to two or more units in close physical proximity to each other in the data center.

For the cooling systems shown in Figure 26 through Figure 29, the design is four of the eighteen CRAH units are redundant. Therefore the design for the electrical power has to be such that loss of any one switchboard or panel does not cause more than four CRAH units to be without power. If the electrical distribution system is 2N, such as shown in Figure 15 or Figure 16, the power could be provided by the system shown in Figure 31 or Figure 32. For these designs, the CRAH units have to be specified for two input sources. Typically the CRAH unit will have a pair of contactors, a selector switch, and a time delay relay to control the power. The selector switch allows the operator to determine which supply is primary and which supply is alternate. The time delay determines how long to wait for the primary source to return before switching to an alternate source. This prevents the contactors from operating unnecessarily, such as during a transfer from utility to generator power.

If it is an existing facility and the CRAH units were specified to be fed by a single source, ATSs can be used as shown in Figure 33. In Figure 33, one of the mechanical distribution switchboards can lose power and only four CRAH units will be without power since the remaining two have ATSs and will transfer to the alternate source.

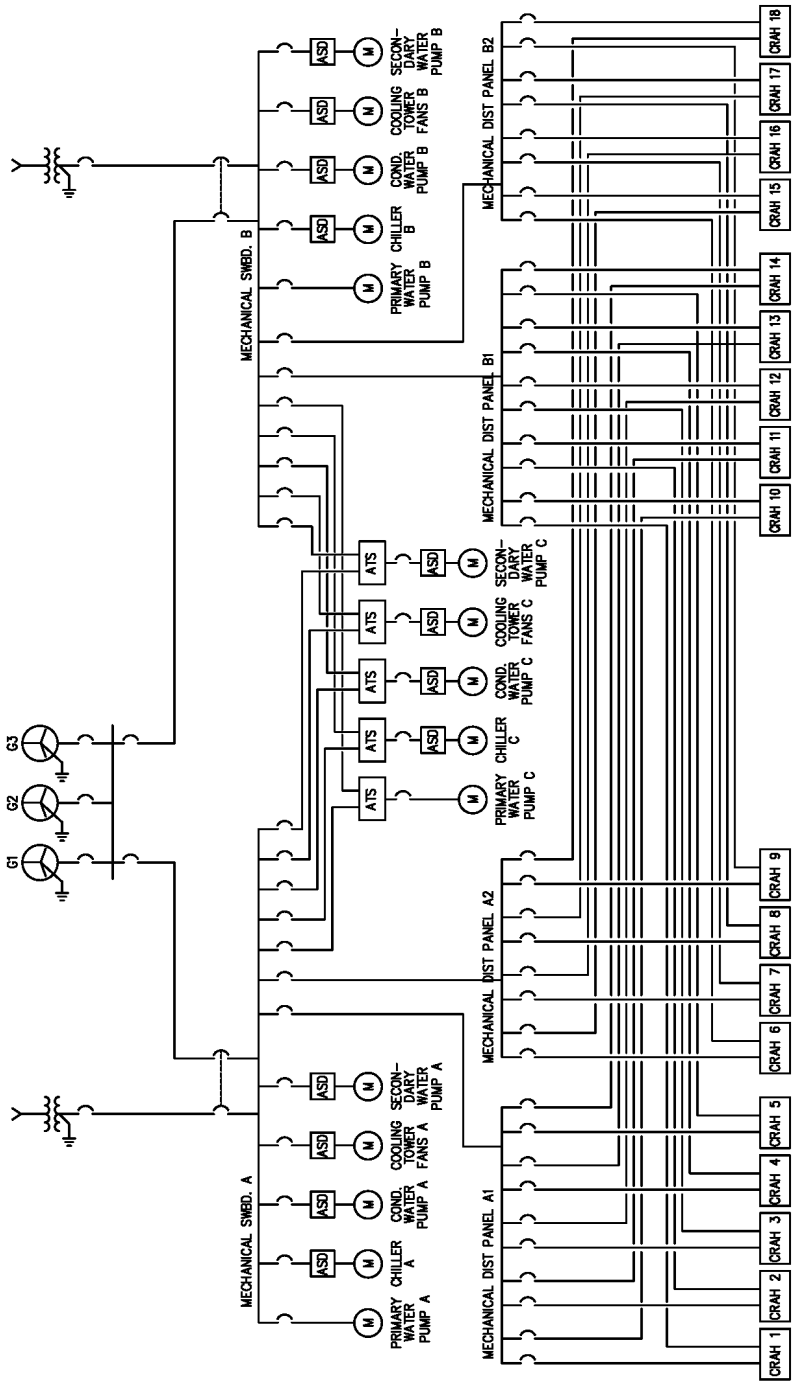

Figure 32—2N electrical system providing power to a 2 out of 3 mechanical system

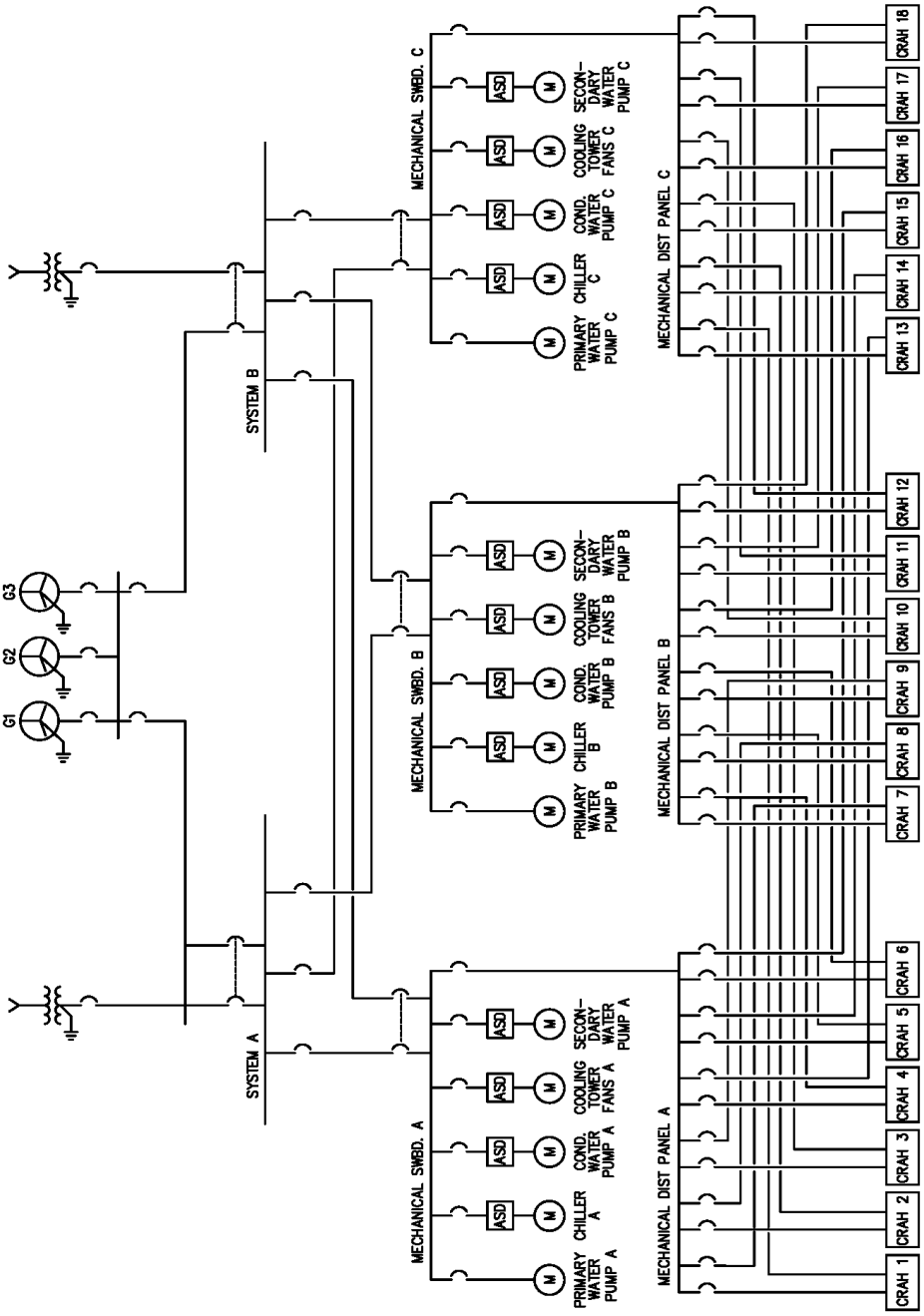

Figure 33—2N electrical system providing power to a 2 out of 3 mechanical system with circuit breaker transfer pairs feeding each switchboard

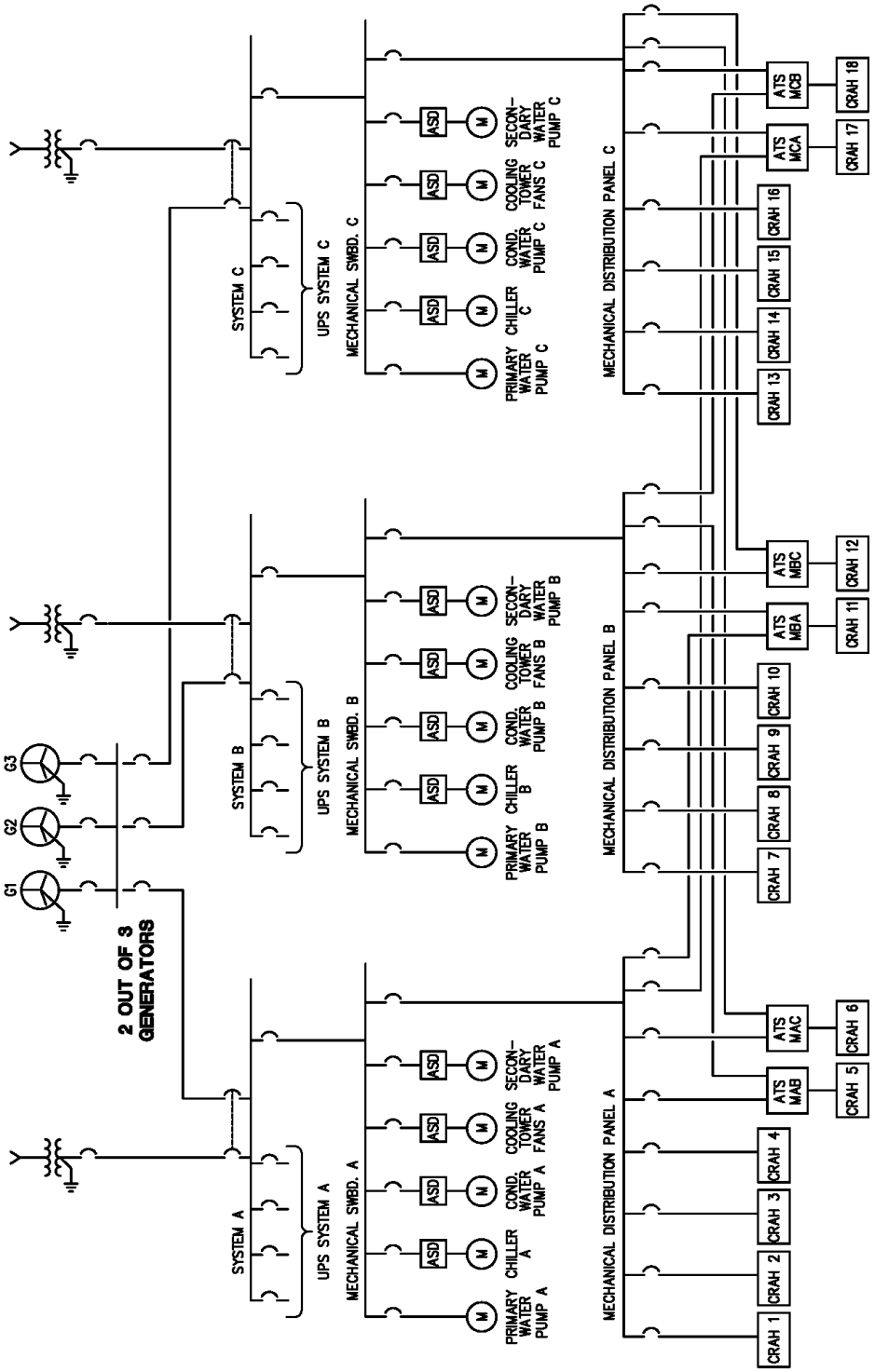

Figure 34—2 out of 3 electrical and mechanical system

9.5 Reliability of the electrical power to critical mechanical cooling system

The reliability of the electrical power to the mechanical cooling is modeled in a similar manner as the power distribution to the IT loads. However, in evaluation of the reliability of the critical cooling system, the reliability of the mechanical equipment that makes up the cooling system and the reliability of the electrical power supplied to it together comprise the reliability of the critical cooling system. When using RBD to analyze the overall reliability of the critical cooling system, the reliability of the mechanical equipment would be combined as a series connection in the RBD with the reliability of the electrical power to it. In the FTA, this is represented as an OR decision at the risk branch. In order for the top level event of a cooling failure, either a mechanical failure OR a loss of power to the mechanical components is sufficient to result in the loss of cooling event.

A word of caution is in order at this point. Reliability analysis is a tool to improve the design and operation of critical facilities. It is only of value as it provides insight that assists in improving the systems and ultimately the overall ability of the critical facility to perform the intended functions. For many designs of the critical cooling systems, there is an order of magnitude (10) or greater difference between the reliability of the mechanical equipment and the reliability of the power supplied to it. Just combining the results of the two RBDs would therefore obscure any insight that could be gained for improving the two systems. So it is often best to keep the two RBDs as separate analysis, but focus the majority of attention on improvements to the less reliable of the two RBDs.

Table 6—Reliability and availability of electrical power to mechanical cooling systems

Name	Description of critical distribution system	MTBF (years)	MTTR (hours)	Inherent availability	Probability of failure
Figure 33 without ATSs	2 of 3 Electrical Swbds feeding (14 of 18) CRAH	5.2	2.78	0.9999389	61.62%
Figure 33	2 of 3 Electrical Swbds feeding (14 of 18) CRAH with ATS for 4 CRAH	70.2	2.00	0.9999968	6.86%
Figure 33 with contactors	2 of 3 Electrical Swbds feeding (14 of 18) CRAH with two contactors in each	147.4	1.20	0.9999991	3.52%
Figure 31	2N feeding 2 of 3 Electrical Swbds with ATS feeding one set of chillers, etc. + (14 of 18) CRAH with two contactors in each	90.7	1.61	0.9999980	5.69%
Figure 32	2N feeding 2 of 3 Electrical Swbds with breaker transfer pairs + (14 of 18) CRAH with two contactors in each	192.3	1.15	0.9999993	2.79%

9.6 Controls for critical mechanical cooling system

The controls required for the mechanical cooling systems used in 7×24 continuous power systems are not the same as systems used in typical HVAC applications for office buildings, etc. The typical BMS used for 7×24 continuous power systems is more robust and often has built-in redundancy.

One of the most important features that is required for 7×24 applications is that failure of the BMS system does not cause the cooling system to shut down. Instead, the cooling system continues to run at the last set-point provided. This may or may not be the case for a HVAC system cooling an office building, as it would depend on the specifics of the design.

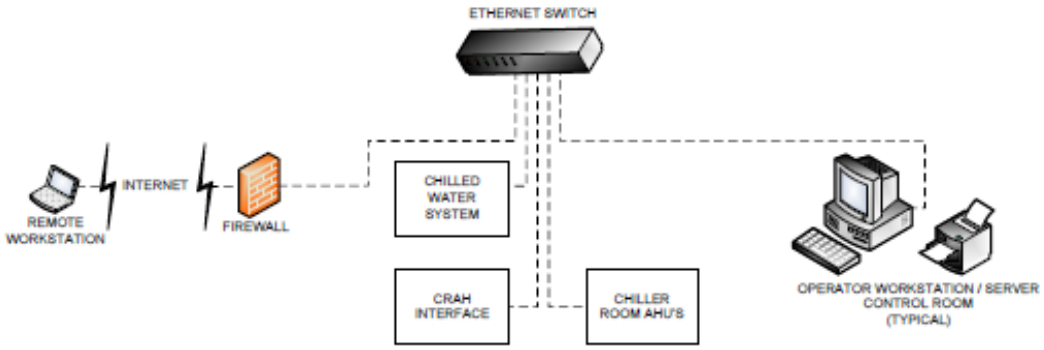

Figure 35—Basic BMS architecture

Shown in Figure 34 is a basic BMS design. Failure of any one of the three controllers may cause loss of HVAC depending on the specific equipment used, the features provided by the BMS, and how it has been programmed.

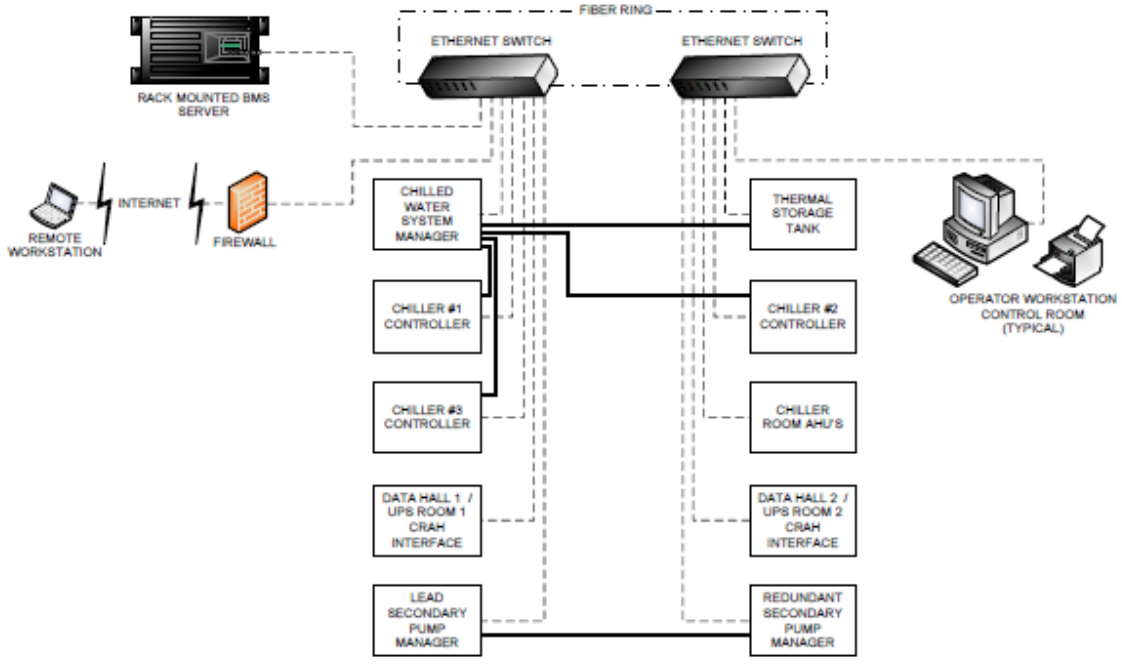

Figure 36—BMS architecture with individual controllers

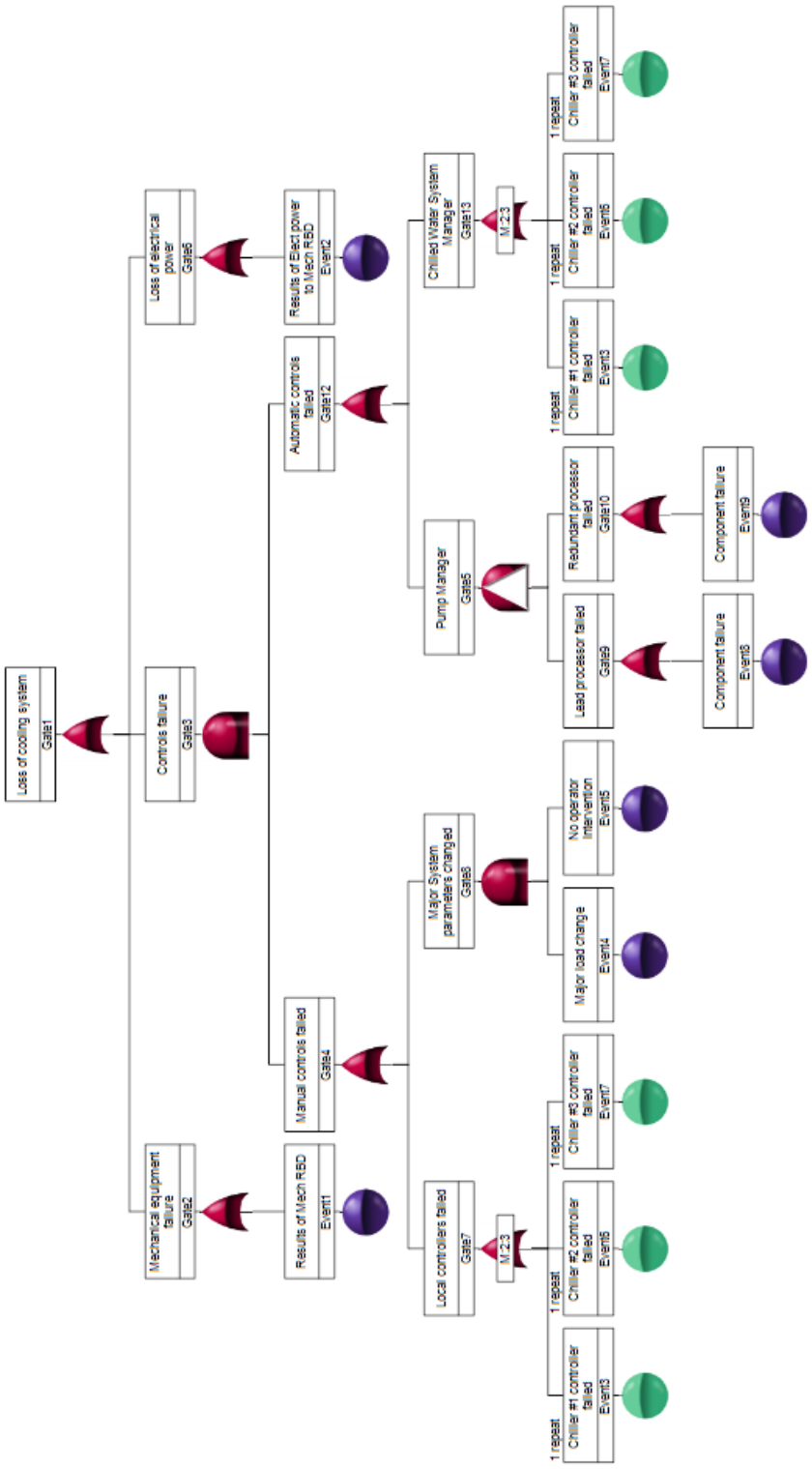

Figure 37—Fault tree for loss of cooling

A typical BMS designed for 7×24 continuous power systems utilizes individual controllers for the chillers, pumps, etc. As shown in Figure 35, there is also a redundant secondary pump manager with a dedicated communication line to keep the data up to date in both managers. Loss of the lead secondary pump manager has no impact on the operation of the cooling system. Loss of chiller #1 controller would cause chiller #1 to operate at the last set-point it was given. If the BMS was not affected by the failure and only the chiller #1 controller failed, the BMS would probably start another chiller, and when it was operating, shift the load off of chiller #1 and shut it down. Each of the controllers is programmed in a similar manner; failure of the controller causes the equipment to continue operating at the last set point provided.

Many designs for 7×24 facilities also include a redundant BMS server, so there are essentially two BMS controllers. In this type of set up, one unit is the master. In addition to operating the cooling system, it continually updates the redundant controller so it always has the latest commands and set-point. This enables the redundant controller to seamlessly take over if the master fails.

Analyzing the controls of the cooling system designed for 7×24 operation can be quite complex. The best approach is often to start with an overview, then drill down into the details of the areas of greatest concern. Figure 36 shows a typical fault tree with loss of cooling system as the event under investigation. For this example, only the central plant cooling system is addressed (not including the interface with the CRAH and AHU) using a control system similar to Figure 35.

This example shows how manual intervention can also be a significant factor in successful handling of a controls failure. For facilities that do not have facility engineers on site 7×24, loss of automatic control would be a more significant failure mode than in a facility with trained operators on site.

10. Commissioning, operations, and maintenance for 7×24 continuous power systems

10.1 Commissioning of 7×24 continuous power systems

As we have shown in the previous section, the designs for the electrical and mechanical distribution systems are critical in achieving reliable operation of 7×24 continuous power systems. However, the best designs can be completely undermined by improper installation of the equipment or equipment/systems that do not operate in accordance with the basis of design for the project. Both of these factors can be addressed by a comprehensive acceptance testing, equipment startup, and commissioning process of the new installation before it is placed in service.

10.1.1 Profile of the failure rate over the equipment life cycle

The bathtub curve shows how the failure rate changes with time over the life cycle of many types of equipment. There is often a period at the beginning where the equipment fails rapidly, usually due to some defect in the material, manufacturing, or installation. This is called the period of infant mortality. After these defects have been corrected, there is usually a relatively long period in which the equipment has a constant failure rate. As the equipment approaches the end of its useful life, the failure rate begins to increase. This is often referred to as the wear-out period.

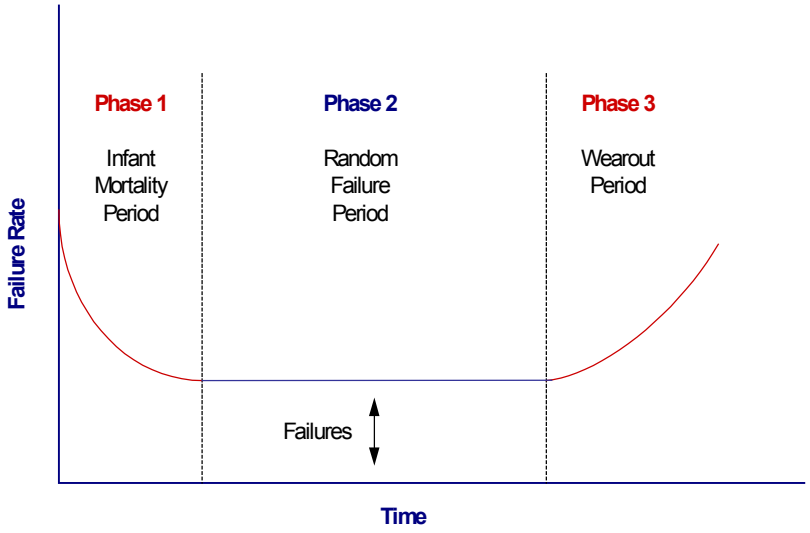

Figure 38—Bathtub curve of equipment failure

The reliability modeling done in this report is based on the assumption that the equipment is in the constant failure rate portion of its life cycle. To get the new equipment and systems past the infant mortality period, burn-in tests for the major equipment, such as generators and UPS modules, are done as part of the factory testing and on-site equipment start up. Then a comprehensive commissioning program is done to ensure all of the system components are properly installed and operating in accordance with the design.

10.1.2 Commissioning of critical electrical distribution systems

The typical sequence for putting critical electrical distribution systems into service is as follows:

1. Checklists are filled out to ensure construction is complete and the equipment is ready for the testing and commissioning program to begin.
2. Acceptance testing is performed on the electrical distribution equipment, such as circuit breakers, transformers, power cables, automatic transfer switches, switchgear, switchboards, motor control centers, and power distribution units.
3. Electrical contractor energizes the electrical distribution system so that power is available for equipment start up.
4. Equipment vendors (generators, UPS modules, ATS, STS, etc.) start up their equipment and make sure it is operational. Burn-in tests, in which the equipment is operated at rated load for an extended period of time (such as 4 h, 8 h, 12 h, or 24 h), are also performed.
5. Commissioning tests are performed on the major components, such as generators, UPS modules, and STS using resistive load (and reactive load for some applications).
6. Commissioning tests are performed on the major systems, such as the transfer from utility power to generator power and on the UPS systems.
7. Load banks are installed on the secondary of the PDUs to provide the rated load for the UPS system design and the heat in the data center rooms for the mechanical cooling systems commissioning.
8. Once the mechanical systems are commissioned, an integrated systems test (IST) is performed with both the critical electrical distribution and critical mechanical cooling system operating at rated load in accordance with the designs.

10.1.3 Commissioning of critical mechanical cooling systems

The typical sequence for putting a water-cooled chilled water cooling system into service is as follows:

1. Checklists are filled out to ensure construction is complete and the equipment is ready for the testing and commissioning program to begin.
2. Contractor for the BMS verifies the inputs and outputs for all of the controls are properly connected and the sequences are programmed in accordance with the specifications and design documents.
3. Once the electrical contractor has energized the electrical distribution system so that power is available for equipment start up, the mechanical contractor flushes the major piping and ensures the proper water treatment has been provided.
4. Equipment vendors (chillers, cooling towers, etc.) start up their equipment and make sure it is operational.
5. The test and balance contractor adjusts all of the valves, dampers, etc. as needed to set the required water and air balance for the mechanical cooling systems.
6. Commissioning tests are performed on the major components, such as chillers, pumps, cooling towers, and CRAH units.
7. Commissioning tests are performed on the major systems.
8. Load banks are installed on the secondary of the PDUs to provide the rated heat load in the data center rooms for the mechanical cooling systems commissioning.
9. IST is performed with both the critical electrical distribution and critical mechanical cooling system operating at rated load in accordance with the designs.

10.2 Operations of 7×24 continuous power systems

The operations staff for a 7×24 facility can vary considerably. A large enterprise data center will have multiple people on-site 7×24×365. A small web hosting facility, on the other hand, may be lights out in which people are on-site only during weekday business hours and to respond to alarms when something happens. The understanding and ability of the individuals can also vary considerably. Many of the large data centers have people who are quite knowledgeable and very experienced in data center operations. Smaller facilities often are staffed by people more knowledgeable on HVAC systems from prior work on high-rise buildings than experienced with data centers.

In all cases, the reliability of the best designed, constructed, and commissioned data center can be undermined if the operations group does not completely understand it and know what to do and what not to do. Human-caused failures are a significant percentage of the root causes of data center failures in actual operation. Therefore training of the staff, providing proper procedures, and ensuring the procedures are followed are all critical elements for reliable 7×24 continuous power.

There has been significant work done in reliability analysis in the area of human-caused failures, primarily by NASA. However, as this time it is still a work in progress.

Practical experience from analyzing data center failures has shown that the failures often occur while some other unusual activity is taking place, such as connecting in new equipment or performing switching to allow for equipment maintenance. Therefore many companies require a critical work authorization in order to perform any work in the data center. The process of analyzing the work to be performed, writing comprehensive procedures, and ensuring the procedures are followed has been one of the most successful tools in eliminating human-caused failures.

10.3 Maintenance of 7×24 continuous power systems

As with all systems that have moving parts, maintenance is required to keep the systems operating properly. IEEE Std 3007.2 provides the recommended practice for maintenance of the electrical distribution system.

American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE) is a very good source of information on mechanical cooling systems.

Annex A

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Arno, R., Friedl, A., Gross, P., and Schuerger, R., "Reliability of Example Data Center Designs Selected by Tier Classification," *2010 IEEE I&CPS Technical Conference Record*.

[B2] Arno, R., Githu, G., Gross, P., Schuerger, R., and Wilson, S., "Reliability of Example Mechanical Systems for Data Center Cooling Selected by Tier Classification," *2010 IEEE IAS Conference Record*.

[B3] Arno, R., Githu, G., Kurkjian, C., and Schuerger, R., "Reliability Modeling of Data Center Cooling Systems," *2012 ASHRAE San Antonio Annual Conference Record S-12*.

[B4] Arno, R., Gross, P., and Schuerger, R., "What Five 9s Really Means and Managing Expectations," *2006 IEEE IAS Conference Record*.

[B5] Gross, P., "Configuration of Large UPS Systems for Super-Critical Applications," *Power Quality Conference Proceedings*, Irvine, CA, 1993.

[B6] Gruzs, Thomas M., "Redundancy Options for Critical Uninterruptible AC Power Systems: Which Type of Redundancy is Best?" International Power Quality 1998 Conference.

[B7] IEEE Std 379™, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.[5]

[B8] Kumamoto, H., and Henley, E., "Probablistic Risk Assessment and Management for Engineers and Scientists," IEEE Press, Piscataway, NJ, 1996.

[B9] Vesely, W. E., et al., *The Fault Tree Handbook*, U. S. Nuclear Regulatory Commission, Washington DC, 1981.[6]

[5] IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

[6] *The Fault Tree Handbook* can be found at the U. S. Nuclear Regulatory Commission website (http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492.pdf).